2019

Successful Operational Cyber Security Strategies for Small Businesses

Wileen Barosy
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Wileen Barosy

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. Carol-Anne Faint, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Dorothy Hanson, Committee Member, Doctor of Business Administration Faculty

Dr. Rocky Dwyer, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Successful Operational Cyber Security Strategies for Small Businesses

by

Wileen Barosy

MBA, Strayer University, 2013

BAS, Miami Dade College, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2019

Abstract

Cybercriminals threaten strategic and efficient use of the Internet within the business environment. Each year, cybercrimes in the United States cost business leaders approximately $6 billion, and globally, $445 billion. The purpose of this multiple case study was to explore the operational strategies chief information security officers of high-technology companies used to protect their businesses from cyberattacks. Organizational learning theory was the conceptual framework for the study. The population of the study was 3 high-technology business owners operating in Florida who have Internet expertise and successfully protected their businesses from cyberattacks. Member checking and methodological triangulation were used to valid the data gathered through semistructured interviews, a review of company websites, and social media pages. Data were analyzed using thematic analysis, which supported the identification of 4 themes: effective leadership, cybersecurity awareness, reliance on third-party vendors, and cybersecurity training. The implications of this study for positive social change include a safe and secure environment for conducting electronic transactions, which may result in increased business and consumer confidence strengthened by the protection of personal and confidential information. The creation and sustainability of a safe Internet environment may lead to increased usage and trust in online business activities, leading to greater online business through consumer confidence and communication.

Successful Operational Cyber Security Strategies for Small Businesses

by

Wileen Barosy

MBA, Strayer University, 2013

BAS, Miami Dade College, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2019

Dedication

This program has been a long journey for me, and I want to thank God, my family, and friends for the strength they gave me to complete this study. This journey was not easy, but I was able to complete it.

Acknowledgments

Completing this doctoral study has been my educational goal. I would like to thank Dr. Carol-Anne Faint, Dr. D'Marie Hanson, Dr. Rocky Dwyer, and all my instructors and classmates at Walden University for all the support and positive feedback. I hope to one day pay it forward. I would like to thank all the participants who participated, finally making this study possible. Lastly, I would thank my family and friends who shared this journey with me. You gave me encouragement when I wanted to give up, pushed me as I wanted to quit, and now I made it to the finish line of my journey. Never underestimate the power you give someone by believing in them.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Cyberattacks against small businesses continue to paralyze company growth due to the invasion into private business and personal data. Small to medium-sized business owners are under pressure to prevent, rather than respond to cyberattacks. Cyberattacks are increasingly detrimental to networks, systems, and users, and are increasing in number and severity globally (King et al., 2018). The ways that small and medium-sized enterprises (SME) share knowledge and conduct electronic business make them a popular target for cyberattacks. SME owners often lack the necessary resources to implement emerging cybersecurity methods and exploit business opportunities (Henschel & Heinze, 2018). Furthermore, SME owners typically lack a cyber-security infrastructure capable of keeping up with cyber-security threats. SME owners face cybersecurity challenges different than those confronting large enterprises. Small business owners use computer systems and the Internet to compete in the technology-infused global e-commerce markets. The purpose of the study was to explore operational strategies chief information security officers (CISOs) of small high-technology companies use to protect their businesses from cyberattacks.

Background of the Problem

Criminals infiltrate businesses through information system hacking behavior (Sieber & Neubert, 2017). However, due to the reach of the Internet, crime committed on the Internet has no geographic bounds (Low, 2017). Cybercriminals continue to target businesses because they have valuable exploitable information. Small businesses store large amounts of sensitive data electronically using outdated and ineffective security

systems, placing the company at risk of cyberattacks. Keeping customers and financial information secure is a constant battle for all organizations (Locke, 2017). With the increased convergence of technologies whereby a user can access, store, and transmit data across different devices in real-time, risks will arise from a lack of appropriate security measures, users not having requisite levels of security awareness, and users not fully understanding how security measures are useful (D'Orazio, Lu, Choo, & Vasilakos, 2017). Small-scale information technology users (SSITUs) remain ill-served by archaic or obsolete cybersecurity practices (Osborn & Simpson, 2017). Therefore, my objective in this study was to explore strategies CISOs of high-technology companies use to protect their businesses from cyberattacks.

Problem Statement

Cyberattacks pose a significant problem for business owners who struggle to protect business and customer private information (Bendovschi, 2015). In 2017, cyberattacks cost the global economy approximately $445 billion (Samtani, Chinn, Chen, & Nunamaker, 2017). The general business problem is organizational leaders place their profitability at risk if they do not have adequate protection from cyberattacks. The specific business problem is CISOs of high-technology companies lack strategies to protect their businesses from cyberattacks.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies CISOs of high-technology companies used to protect their businesses from cyberattacks. The target population consisted of CISOs from three small businesses operating in

Florida who successfully protected their business from cyberattacks. The CISOs were appropriate participants for this study due to their knowledge and expertise in preventing cyberattacks. The implications for positive social change could provide customers with a safe and secure environment for communicating and conducting electronic transactions.

Nature of the Study

I conducted a qualitative multiple case study to explore strategies CISOs of high-technology companies use to protect their businesses from cyberattacks. I considered quantitative, qualitative, and mixed method approaches for this study. Researchers use quantitative inquiry to test hypotheses using variables and considering relationships or comparisons (Boersma et al., 2016). I did not select the quantitative approach because I was not seeking to explain phenomenon based on a hypothesis. A qualitative researcher conducts interviews using open-ended questions to learn about participant perspectives, decision making processes, and experiences (Yin, 2014). I selected the qualitative method as a means of interviewing participants and gaining detailed information by asking *how* and *what* questions. Mixed method researchers apply a combination of quantitative and qualitative methods (Sim, 2017). The mixed method approach was not appropriate because it includes the quantitative method.

The three qualitative research designs I considered for this study were phenomenological, ethnographic, and case study designs. Phenomenological researchers explore subjective perceptions of lived experiences of an individual or group of people connected to a single phenomenon (Johnston, Wallis, Oprescu, & Gray, 2017). The phenomenological design was not appropriate for this study because I sought to explore

beyond the scope of lived experiences and included additional data to understand the phenomenon. Ethnographic researchers explore human behaviors within a culture or group (Puttick, 2017). Ethnographic research was not appropriate for this study because I did not explore human culture or behaviors within a specific group. A case study researcher investigates a phenomenon within a specific context to address the research questions (Yin, 2014). A case study researcher uses triangulation to investigate a phenomenon. My approach included interviews, a review of existing company documents, and a review social media sites. A multiple case study researcher investigates multiple businesses to understand business leader behaviors. A qualitative multiple case study design was appropriate for this study because I conducted semistructured interviews, explored company websites, and reviewed social media portals to gain a thorough understanding of cyberattack prevention.

Research Question

The overarching research question for this study was: What strategies do CISOs of high-technology companies use to protect their businesses from cyberattacks?

Interview Questions

1. What strategies are you using to secure your business from cyberattacks?
2. What are the key challenges to implementing your operational strategies for preventing cyberattacks?
3. How do you address the key challenges to implementing your successful strategies to mitigate cyberattacks?
4. How do you assess the effectiveness of the strategies you implemented to

achieve the desired outcomes?

5. How long has your business been in existence?
6. What type of training do you have in place for your employees about cyber-attacks?
7. What type of cyberattacks strategies would you like to implement but have not implemented?
8. What additional information on cybersecurity strategies would you like to provide?

Conceptual Framework

The conceptual framework for this study was the organizational learning theory developed by Chris Argyris in 1974. Argyris (1976) explored the concept of organizational learning and its impact on a company's growth. Argyris focused on single-loop and double-loop learning. Single-loop learning encourages participants to learn to perform, as long as the learning does not question the fundamental design, goals, and activities of their organization (Argyris, 1976). Double-loop learning encourages participants to ask questions about changing fundamental aspects of the organization (Argyris, 1976). The tenets of organizational learning theory include (a) systems thinking, (b) personal mastery, (c) mental models, (d) building shared vision, and (e) team learning. Argyris (1993) promoted the concept of integrated problem-solving drawing on individual contributions that add unique talent and ingenuity into decision-making processes. The focus on collaboration provides a useful model from which to understand how to integrate ideas to understand applied business concepts, fostering

improved business performance. As applied to my study, organizational learning theory provided for a deeper understanding of operational strategies within the cybersecurity industry.

Operational Definitions

Badware: Badware is a software installed on a computer which can be harmful in one's system but totally harmless in another without knowledge or control *(*Han, Liu, Han, Jia, & Lei, 2018).

Chief information security officer (CISO): The CISO is an individual who is responsible in an organization to identify the information security concerns in information technology (IT) outsourcing (Dhillon, Syed, & de Sá-Soares, 2017).

Cyberattacks: Cyberattacks are an attempt by hackers to damage or destroy a computer network (Page, Kaur, & Waters, 2017).

Cybercrimes: Cybercrimes are crimes committed using malware and badware with no viable mechanism (Rahman, 2017).

Data security: Data security is the provision of real-time security petabytes of data which is important for cloud computing (Chang, & Ramachandran, 2016).

Data security breach: Data security breach is a privacy and security breach which occurs from within a cloud service provider (CSP) as well as data states: data at rest, while transferring data, enquiring data, and processing the data (Chakraborty, Sharma, & Ranjan, 2016).

Organizational learning: Organizational learning which is a predictor of knowledge transfer in an operational environment (Liu, 2018).

Risk management: Risk management is the forecasting and evaluation of financial risks together with the identification of procedures to avoid or minimize their impact (Rostamzadeh, Ghorabaee, Govindan, Esmaeili, & Nobar, 2018).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions in research help improve the quality of data (Xie, Hong, Laing, & Kang, 2017). In this doctoral study, I made two assumptions. The first assumption was that the data collection process would provide ample information to support a thorough investigation of the phenomenon. The second assumption was that through the interview process, participants would recall significant information to ensure the quality of the investigation. In both cases, these assumptions proved true through diligent data collection processes and the use of probing questions.

Limitations

Limitations represent potential weaknesses of the study (Eaton & Millar, 2017). The one limitation in this study was the lack of generalizability of the findings to all populations in all industries. While the information gathered in my research may be the experiences of few, the findings may prove appropriate and applicable to similar businesses in the cybersecurity industry.

Delimitations

According to Sheperis, Young, and Daniels (2016), delimitations are the boundaries of the research study. First, I delimited this study to small business owners

located in the southern United States. Second, I delimited the study to CISOs of high-technology companies who were available for face-to-face interviews.

Significance of the Study

Contribution to Business Practice

Technology can help SME owners provide greater efficiency. SME owners utilize technological innovations to streamline business process and implement effective policies. CISOs are senior-level executives responsible for developing and implementing an information security program, which contains policies and procedures intended to protect enterprise communications, systems, and assets from both internal and external threats of cyberattacks (Bauer & Bernroider, 2017). Small businesses are not only a target of cybercrimes, but also main targets through which cybercriminals place the privacy of consumers at risk of identity theft (Qabajeh, Thabtah, & Chiclana, 2018). Organizations need to implement appropriate defensive measures to safeguard their business operations from any attacks. Systems security is essential for the efficient operation of all organizations (Baldwin, Gheyas, Ioannidis, Pym, & Williams, 2017). Security, trust, and privacy are unending challenges for organizations that adopt cloud computing and big data (Chang, Kuo, & Ramachandran, 2016). Findings from my study may have a significance for small business leaders looking to prevent and mitigate costs from cyberattacks. The findings may also provide small businesses with operative strategies to protect their business against a cyberattack that might decrease derivate costs and increase consumer confidence.

Implications for Social Change

Information and communications technology are expected to become ever-more embedded in the economy and society, bringing both benefits and risk-related costs (Hughes, Bohl, Irfan, Margolese-Malin, & Solorzano, 2016). This study's implications for positive social change include increasing the sustainability of information technology in businesses. The findings in this study may help SME owners understand cybersecurity strategies and invest in security to protect customers' personal information. The public may experience greater trust in the safety of transactions, leading to improving the use of Internet services to conduct daily business and activities without having to incur the costs from cyberattacks.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore the operational strategies CISOs of high-technology companies use to protect their businesses from cyberattacks. The specific target population consisted of high-technology companies operating in Florida who have successfully protected their businesses from cyberattacks.

The literature review consisted of 236 sources of which 185 (95%) were current peer-reviewed journal articles published no earlier than 2015. The following topics appear in the literature review: *cyberattacks, Chief Information Security Officers, information security risk, cyber impact,* and *privacy and protection*. The databases and journals I used to develop the literature review include Google Scholar, IEEE Xplore Digital Library, Science Direct, *International Journal of Robust Security, The Journal of Applied Behavioral Science, Organizational Dynamics, Information Management and*

Computer Security, European Journal of Economics, Journal of Cleaner Production, Production and Operations Management, International Affairs, Computers and Security, The Learning Organization, and Nonlinear Control, Human Resource Management Journal, Neurocomputing, Information Resources Management Journal, Information and Computer Security, World Review of Entrepreneurship, Management and Sustainable, Development, Strategic Management Journal, and *Journal of Technology Transfer*. A review of the literature enhanced my understanding of the strategies CISOs of high-technology companies use to protect their businesses from cyberattacks and the overall impact of cyberattacks on businesses.

Organizational Learning Theory

Organizational learning theory served as the theory comprising my study's framework. Organizational learning theory is a concept of everyday practical coping guided by internalized sensitivities and predispositions (Rezaei, Allameh, & Ansari, 2018). Single-loop learning and double-loop learning are two essential tenets of organizational learning. Argyris and Schon (1978) developed these two concepts and emphasized that interaction often goes well beyond defined organizational rules and procedures. Argyris and Schon has made a significant contribution to the development of the organizational learning theory. Rezaei et al. (2018) found that knowledge creation had a positive effect on organizational learning. Ideally, the effective organization should have a two-loop model of training and function in the business.

The single-loop and double-loop model provides a basic understanding of change management as a behavior change tool. Argyris (1976) argued the single-loop learning

encourages participants to learn to perform as long as the learning does not question the fundamental design, goals, and activities of the organization. Wang et al. (2018) argued that an efficient single-loop strategy is design in the presence of uncertainty. Single-loop learning theorists have suggested that organizations avoid mistakes and double-loop learning, and that they correct or change the underlying cause of the business problem (McClory, Read, & Labib, 2017). Single-loop occurs when a process changes because of a known deficiency (Argyris, 1996). The goal of single-loop learning is to provide feedback to enhance the efficiency of the process change. Individuals will only be creative and reflexive to avoid being singled out in the organization (Argyris, 1976). The problem with using single-loop learning is that the method does not provide the feedback which could help the efficiency of the process.

Leaders can use double-loop learning theory to reexamine problems organizations face to add efficiency to the process. Double-loop learning occurs by changing the fundamental principles of the actions in the process change (Argyris, 1976). Argyris argued that double-loop learning encourages participants to ask questions about changing fundamental aspects of the organization. Matthies and Coners (2018) argued that organizations learn from past failures and successes. The implementation of double-loop learning also enhances the communication between management and the employee (Argyris, 1976). In contrast to double-loop learning, single-loop learning is used to solve problems symptomatically (Argyris, 1976). Perhaps the impact of double-loop learning and the process of interchange may justify the complexity and dynamics of changes in policies and strategies for learning. Double-loop learning is an educational concept and

process that involves teaching people to think differently about their own assumptions and beliefs. The double-loop theory may help individuals develop new skills, and it allows the educator to create opportunities for individuals to understand and rethink why they lead and how they lead individuals in businesses. The implantation of double-loop learning increases the communication between management and the employees learning to correct errors in a process (Argyris, 1993). The results of double-loop learning could increase the effectiveness of the monitoring of decisions by business leaders.

The vision of an organization's leadership permeates the workplace and is manifested in the values and goals of the business leaders. The development of this vision will start with the business leaders' knowledge of how to deploy strategic alliances (Simonin, 2017). Once business leaders obtain information, assistance, and qualities, the managers will have the necessary information to interact and allow business leaders to get the best out of their people from a single view to an organizational view (Kuo, Lin, & Lu, 2017). Having a clear vision allows business leaders to provide their firms with competitive advantage, but longitudinal results in some studies have indicated that some types of obvious content provide more enduring advantage than others do (Harrigan & DiGuardo, 2017). Business leaders should offer motivation and opportunities to build an effective long-term financial incentive and not just focus on the money (Delery & Roumpi, 2017). Businesses can tap their insubstantial assets to grow their cost in the business help business leaders transition from their present way of working to the desired way of working.

Organizational learning theory highlights the intricacies of personal experience and the influence of experience on workplace behaviors. Organizational learning theorists are motivated by the observation that organizational leaders learn by making inferences from experience (Greve & Seidel, 2014). Organizational learning involves gathering information, analyzing the information, and learning from failure (Dahlin, Chuang, & Roulet, 2018). Zhai et al. (2018) conducted research showing 324 SMEs discussed the relationship between entrepreneurial orientation, absorptive capacity, environmental dynamism, and corporate technological innovation performance. Zhai et al. suggested that the relationship between entrepreneurial orientation and innovation performance is significantly positive based on the moderation model.

The driving force of business theory is in the application of theoretical tenets. Organizational learning theory has five main contextual dimensions (a) organizational context and role, (b) geographical and spatial context, (c) social context and teams, (d) institutional cultural norms, and (e) temporal dynamics (Wright et al., 2018). According to the knowledge-based view of organizational learning theory, knowledge is embedded in individuals and combined with organizational routines to generate innovative activities (Grant, 1996). Argyris (1976) explored the concept of organizational learning and its impact on a company's growth. Argyris found no alignment between the dynamic theories of organizational knowledge when learning involves various forms of employee and entrepreneurial movement through a change in ownership. The disruption in leadership poses challenges to reaping benefits from consistent management approaches.

Organizational learning is a product of organizational inquiry. Organizational learning is how organizational leaders create and organize knowledge related to their functions and culture. Organizational learning occurs in all the organizational leaders' activities. The organizational learning theory involves developing, retaining, and transferring knowledge within an organization (Qi & Chau, 2018). The goal of organizational learning practitioners is to recreate changes or interventions (Pisano, 2017). Organizational leaders who are capable of maintaining the ability to self-adapt can flourish. When business leaders process organizational learning, the cybersecurity professional will interact with other members of the organization and productive learning takes place.

Communication within an organization, generally considered an asset, can hinder progress based on defensiveness and refusal to examine one's own attitudes and contributions toward a problem. Organizational learning theorists use the approach to moderate the relationship between managerial ties and capturing opportunities (Li, Chen, Liu, & Peng, 2014). Baumgartner and Rauter (2017) connected three distinct but complementary dimensions of strategic management, as viewed from the perspective of sustainability, to encourage the integration of sustainability issues into corporate activities and strategies. Capacity development is particularly relevant in dealing with issues such as cybersecurity.

The competitive advantage of learning. The organizational learning theory applies when a company adopts new principles and paradigms that create a competitive advantage. The goal of organizational learning theorists is to effectively change the work

environment (Nordin, Kork, & Koskela, 2017). The real world is costly for experimentation, failing market-facing tests might jeopardize the organizational brand and reputation (García-Sánchez, García-Morales, & Martín-Rojas, 2018). Increasing innovation may allow organizations to gain a competitive edge and adapt organizational designs to apply organization knowledge to emerging business problems.

Organizational learning theory was appropriate for this study primarily because my intent was to understand behaviors within an organization that support developing and sustaining competitive advantage. Pawlak and Barmpaliou (2017) presented the theory as an underpinning of cybersecurity capacity building, the emergence of a principle-based approach to capacity building in cyberspace with a sustainable outlook towards closing the *cyber capacity gap*. To ensure the sustainability of efforts, organizations could establish methods and instruments focused specifically on closing gaps. CISOs could encourage higher-order learning during advanced system development. Organizations would improve their chances of success in a changing and competitive world by integrating appropriate methods and goals.

Theories Considered but Not Used

Transformational leadership. I considered using transformational leadership (Burns, 1978) as a guiding concept, but did not use it given my intent to look beyond leadership style alone as a factor in reducing cybercrimes in organizations. Transformational leadership is defined as a social process in which members of a group or organization influence the understanding of internal and external events, the choice of goals or desired outcomes, the organization of work activities, and the individual

motivation and abilities (Frieder, Wang, & Oh, 2018). Transformational leaders moderate the indirect effect of employees' personality traits on their job performance via enhanced perceptions of meaningfulness at work (Frieder et al., 2018). Additionally, transformational leaders moderate the relationship between proactive personality and work engagement, but only when employees have a growth mindset (Caniëls, Semeijn, & Renders, 2018). Transformational leaders often work toward changing the organizational culture through the implementation of new ideas (Northouse, 2016). Transformational leaders establish behaviors that develop trust and organizational views.

Transformational leaders seek to influence relationships within an organization. The transformational leader mediates mechanisms that could exist in the relationship between transformational leadership and organizational performance (Para-González, Jimenez-Jimenez, & Martínez-Lorente, 2018). Transformational leaders show integrity and demonstrate how to develop a robust and inspiring vision of the future (Ashford, Wellman, Sully de Luque, De Stobbeleir, & Wollan, 2018). Transformational leadership was not an appropriate framework for this study because I did not explore the influence of leadership style on cyber attack prevention; rather, the tenets of organizational learning provided a strong foundation to explain business stakeholders' behaviors in promoting a safe and secure work environment.

Situational leadership. Business leaders may have a flexible approach to resolve situational problems arising at work to build an effective organization. Hersey and Blanchard (1969) argued the effective leadership rests in the appropriate balance of task and relationship behaviors. Situational leadership is a very influential leadership model

that enables leaders of all kinds. Situational leadership refers to when the business leader of an organization must adjust to the interaction between person-centered leadership by professional leaders (Lynch, McCance, McCormack, & Brown, 2018). Leadership depends on each situation and no single leadership style may be the best (Finkelstein, Costanza, & Goodwin, 2018). A good business leader will be able to adapt themselves from the leadership to the goals or objectives accomplished (Trotter, Salmon, Goode, & Lenné, 2018). The situational leadership theory was expressed to overcome the weaknesses of traditional leadership that were not suitable for some situations that business leaders faced in the organization (Müller et al., 2018). Situational leadership theory was not an appropriate framework for this study because the process of learning is accumulative and not situational; thus, organizational learning theory was appropriate for the study.

Contingency theory. Effective business leaders know how to frame their ideas and provide direction to employees on how to satisfy the organization's mission. Effective business leaders also form relationships based on mutual trust. Fiedler (1958) argued that there is a direct correlation between the traits of a leader and the effectiveness of a leader. A business leader is a person who directs and coordinates the work of group members (Fiedler, 1967). According to Fiedler, leadership traits helped in a certain crisis and so the leadership would need to change given the new set of circumstances.

Fiedler's contingency theory stated that effective leadership depends not only on the style of leading but on the control over a situation. Contingency theorists claim that there is no best way to organize a corporation, to lead a company, or to make decisions

that trace megaproject performance to variation (Gil & Pinto, 2018; Northouse, 2018). Fiedler's contingency theory is valuable for helping a company foresee the value of a business leader within a given situation before assigning the employee on the job. Contingency theory was not an appropriate framework for this study because I did not seek contingent relationships to explain behavior. Rather, I sought to understand behavior in terms of organizational learning strategies.

Cyberattacks

Networks are vulnerable to interruption by hackers and cybercriminals. The definition of a *cyberattack* is an attempt by hackers to damage or destroy a computer network or system connected to the Internet (Škrjanc, Ozawa, Ban, & Dovžan, 2018). A cyberattack is considered mistreatment of computer systems, technology-dependent enterprises, and network systems (Zhang, Wang, Liu, Ding, & Alsaadi, 2018). For example, cyberattacks have challenged existing electric utility cybersecurity standards to protect critical assets, their integrated dependents, and public safety from cyber threats (Smith et al., 2016). Cybercrime is a growing and insidious problem for small business owners, and owner efforts to encourage universal access to information technologies fail because some business leaders lack cybercrime or IT knowledge to prevent related problems (Jayakar, 2018). Cybercrimes are a phenomenon that, if ignored, could have unlimited damage potential for business privacy, finances, and integrity. Cyberattackers use malicious code to modify computer code and data, causing disruptions that can compromise data and lead to cybercrimes, such as data and identity theft (Burnap, French, Turner, & Jones, 2018). Cyberattacks continue to plague businesses, requiring

business owners to have well-crafted security strategies in place to prevent security breaches.

Cybercrimes can cost businesses billions of dollars. For example, a serious cyberattack caused confirmed physical damage to Sony. Sony suffered an estimated loss of $20 million in revenue, and a $32 billion loss was incurred as a result of losing control of customer data (Hou, Gao, & Nicholson, 2018). After this incident, cyber security at Sony began a process of preventing another attack (Zetter, 2014). Sony implemented a moving target defense to mitigate cyberattacks. Moving target defense is a type of security technology involving the IT infrastructure changing its form actively to prevent various cyberattacks (Park, Woo, Moon, & Choi, 2018). Preventing cyberattacks, especially repeated attacks, is important to all businesses. Business owners try to keep their data secure, but hackers find ways to intercept private, personal data which involves investments of millions of dollars on behalf of customers, creating vulnerabilities to customer personal accounts.

Business owners cannot afford cyberattacks. Cybersecurity professionals need to have a well-crafted security strategy in place to prevent future attacks. The Internet represents one of the most important drivers of innovation, growth, and competitive advantage for national and international economies. Cyberattacks play an increasingly important role in critical infrastructure manipulation, for government security, and consumer privacy (Ding, Han, Xiang, Ge, & Zhang, 2018).

Access to business funding is one of the most effective ways to enhance the resilience of SMEs. The SMEs are an important part of the nation's economy, but their

owners often do not view themselves as targets for cyberattacks, creating a significant weakness to the security of the business (Small Business Association, 2017). The rising costs of cybersecurity render businesses ill equipped to sustain operability, and these costs are estimated to climb rapidly.

Every government is reliant on independent countries to appropriately manage their own cybersecurity issues. The U.S. government recognizes risk management information systems in the developing world; and is needed to improve performance and to impact users of information systems (Kaban & Legowo, 2018). The global business environment must promote online involvement while ensuring the system is not creating undue risks to patrons around the world.

Collecting and assembling data is financially taxing; and increasing data collection efforts could carry the risk of reducing the available resource program an organization has in place. Some companies are creating dynamic methods to secure their organizations. Digital Defense's innovative and leading-edge information security technology helps businesses with a protection-sensitive data and eases the problems associated with information security. Digital Defense, Inc. provides security assessments, coupled with a deep background in security training for governmental and non-governmental organizations (Cabaj, Domingos, Kotulski, & Respício, 2018). The Ponemon Institute (2015) is also a well-known resource for CISOs and other security experts. SecrED is an industry-recognized training program that Ponemon Institute uses to help organizations create a culture of security across the United States. The Ponemon blog provides up-to-date information affecting CISOs government issues, and insider

threats. In 2015, the Ponemon Institute reported its analysis of the cost of all cybercrime for a variety of 58 U.S. organizations, both public and private. Ponemon reported that annual costs of cybercrime doubled since 2010, which averaged $6.5 million (Ifinedo, 2018). One method used by business owners is to develop a strong security policy. Each business requires a policy and procedure to align with the assets of the business. Implementing a policy and procedure could create a safe and welcoming environment for the individuals in the business.

Social media use within the workplace is a common entry point for cyberattacks, and organizations know little about how to actually manage social media risk. A survey data from 98 risk-management, audit, and finance professionals, showed that the extent of organizations' social media use increases the actual risk of social media use (Demek, Raschke, Janvrin, & Dilla, 2018). Organizational information protection initiatives could increase over time as professionals become more comfortable with information management strategies (Felo, Kim, & Lim, 2018). Organizations with a more widespread social media policy could have more extensive training and technical controls. Few organizations are adopting social media policies as opposed to operating a formalized risk management process. This limitation accentuates the potential consequences associated with cybercrime.

Chief Information Security Officers (CISOs)

The CISOs are increasingly finding information security strategies and functions that are no longer adequate when dealing with a progressively more dynamic cyber risk environment. The CISOs could provide craft training and learning principles to clearly

influence positive change. The CISOs in the organization should update and create some risk-based choices rather than applying control in a sensitive manner. The CISO directs the planning and implementation of the enterprise's IT system, business operation, and protections against security breaches and vulnerability issues that occur in the business (Hasbini, Eldabi, & Aldall, 2018). The CISOs perform and oversee the functions and activities that occur in the organization and do not focus only on unauthorized access to the organization. The CISOs are also responsible for auditing the existing system while guiding the management of security policies and procedures, activities, and standards. A CISO must have exemplary interpersonal and written communication skills, solid knowledge of electronic and site security issues, and an understanding of the business environment, stakeholders, and working networks.

Cybersecurity professionals must lead in task accomplishment and lead with integrity. Cybersecurity professionals need to have a clear understanding of their cybersecurity human capital skills and abilities to ensure protection against threats to information systems. Cybersecurity professionals need to focus on the importance, difficulty, and timelessness that connect cybersecurity knowledge in the discipline (Parekh et al., 2018). The CISOs must keep abreast of any new developments to avoid costly mistakes and determine what actions they should carry out for the business infrastructure at the given time. In a competitive organization, a set of skills are needed for CISOs (Whitten, 2018). The CISOs must understand the effect attacks have on society and the environment as vital to realizing sustainability. The CISOs should protect their organization against cyberattacks to potentially increase the confidence resulting in

economic wealth.

The CISOs should partner with other organizations to understand their needs and different strategies to prevent future attacks. Organizations are growing more dependent on digital innovation and require individuals who work within the organization to meet different challenges (Gustafsson & Jarvenpaa, 2018). One of the biggest challenges facing leaders is to position the company securely and enable organization adaptability in the face of increasingly dynamic, demanding, and high-risk environments. Cybersecurity professionals need to distinguish various forms of cyberattacks.

The use of the Internet has changed the decision-making process through changes in communication patterns in some businesses. According to Bashir, Wee, and Guo (2017), *Cybersecurity Awareness Week* is a competition with measures of personality, interests, culture, decision-making, and attachment styles. Bashir et al. examined individuals, from self-proclaimed hackers to non-hackers and cybersecurity employees versus students, in an exploratory study designed to identify the personalities of cybersecurity competition members. The increase of hacking behavior has sparked a debate about how online communication affects social relationships. The Internet releases us from geographic bounds and brings us together to discuss topics, and what binds the public in this domain is the access to the Internet (Bashir et al., 2017). The Internet is the tool we use to interact with one another and to engage in new challenges. The internet is not only affecting our lives but also mentally altering our brains which heightens conflicting interest in the workplace.

Company leaders apply various strategies to approach cyber breaches. According

to Attaran and Woods (2018), personal demonstrations from business owners help cybersecurity professionals focus on leadership development programs for coaching leadership skills and practices. Communication is fundamental for leadership to function more efficiently, but the communication skills and other skills could help leaders change over time because of the infrastructure necessary for Internet connectivity.

Security Awareness Training

Security awareness training focuses on communicating and enforcing security policies. Security awareness training is an effective way to prevent a cyberattacks against small business (Fellnhofer, 2018). Information security policies should include training to protect the integrity of the organization. Fellnhofer indicated that the majority of threats arrive at the staff inbox through phishing scams and other social engineering attacks. Training business leaders to defend against phishing, ransomware, and malicious websites is a necessary component of a business digital security strategy. Training business leaders on how to defend against phishing can help businesses reduce the risk of cyberattacks (Fellnhofer, 2018). Businesses of any size require sufficient cybersecurity measures, and appropriate training to inform employees of cybersecurity risks and best practices.

Business leaders could find a way to protect critical information to gain a competitive advantage in the workplace. According to Tadesse and Murthy (2018), 71% of all data breaches affected companies with fewer than 100 people on the payroll. Ransomware is the fastest growing malware threat and accounts for the majority of extortion based malware causing billions of dollars in losses for organizations around the

world (Thomas & Galligher, 2018). Small business attacks are increasing because they present cybercriminals with a way to access the business leader's information and personal data. Small business tends to have insufficient online security (Carr, 2016). Also, small businesses are doing more online transactions and interactions through cloud services.

Cloud computing is one of the latest strategies in computing. Understanding malicious websites is a necessary component of a business digital security strategy because cloud computing experiences increased popularity, but may pose significant challenges to cybersecurity (Kumar, Raj, & Jelciana, 2018). Cloud computing is used directly and indirectly by businesses and if any breach occurs in cloud computing, a company may experience mounting and lasting ill-effects.

According to the Symantec Corporation, small or medium-sized businesses that experienced cyberattacks, lost an average of over $180,000. Symantec is recognized as one of the largest civilian threat collection networks in the world. Symantec Corporation tracks over 700,000 global adversaries and records from 98 million attack sensors around the world (Symantec Corporation, 2017). The utilization of innovative technology makes collaboration easier for businesses, and business owners should create financial and operational strategies for future impact with data analytics (Wang, Kung, & Byrd, 2018).

Implementing and using a business continuity plan (BCP) helps cybersecurity professionals in the organization understand the risks associated with IT systems and provides solutions to potential security problems. A more efficient business continuity input process, immediate situational awareness for use of progressive planning, and

streamlined analyses for generation of reports for cybersecurity professionals may significantly protect the integrity of organizations (Clark & Guiffault, 2018). By using a consistent process, business continuity management may provide a supportive framework for IT systems. In essence, the organizational structure for business continuity management includes covering the roles of the leaders, identifying the tasks and responsibilities of internal resources, and creating structures to document, test and execute disaster recovery and employ IT contingency plans.

The Security and Exchange Commission (SEC) protects investors worldwide. The US SEC has sanctioned broker-dealers (BDs) and registered investment advisers (RIAs) to officially address issues when security breaches occur, also to determine whether the SEC is imposing a strict liability approach. The SEC agreed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals and thousands of organizations (Rubin & Xu, 2016). Cybersecurity attacks against the SEC led to the implementation of strategies designed to block possible future cyberattacks on businesses. Information security has increased public consciousness due to the universal nature of data breaches, spanning from attacks on small business companies to individual losses on a personal computer. According to Rubin and Xu (2016), strategic cyber intelligence can substantially reduce risk to companies' valued assets and supports due diligence. The SEC goal is to collect information on the state of cyberattacks among small businesses, understand cybersecurity risks, and expose the challenges faced by smaller businesses that could undermine company security.

Information Systems Security Risk

Operating information systems is a critical part of any business that wants to compete in the business world. Some businesses use information systems at all levels of operation to collect, process, and store data. Management gathers and distributes data in the form of information required to carry out the daily operations of the business. The concept of a project-oriented business consists of three segments (a) values, (b) structures, and (c) people (Gemünden, Lehner, & Kock, 2018). The above three segments are ideally based on a range of management disciplines such as (a) the orientations in the value segment developed in strategic management and innovation management; (b) the foundations for the design of the sociotechnical artifacts in the structure segment of organizational design, planning and controlling, the systems theory; and (c) the foundations for the elements of the human side come from organizational behavior, human resource management, and knowledge management theories (Gemünden et al., 2018). Organizations need to understand the value of organizational behavior, human resource management, and knowledge management theories.

Compliance by cybersecurity professionals could provide organizations with confidence to focus on mitigating external threats. The goal of each business owner should be to function in the *organizing stage* of the *maturity cycle*. There are many reasons for a business to flourish or close. Organizational disappointment is inevitable as a business leader experiences business failure due to harmful cyberattacks. However, organizational disappointment may be within the control of the business leaders. Malicious attackers frequently breach information systems by exploiting disclosed

software vulnerabilities (Biswas & Mukhopadhyay, 2018). The cybercrime prevention and response process must start with the human factors that contribute to cybersecurity vulnerabilities and risk (King et al., 2018). Vulnerability analysis is a vital part of effective industrial risk evaluation (Abdo, Kaouk, Flaus, & Masse, 2018). Organizations should create and check incident management plans to respond to security breaches immediately. Cybercriminals are professional at hijacking identities. In some cases, the attackers can upsurge a hacked user's access within a system, leading to the identification and inappropriate exposure of sensitive information. The integration of computing and communication capabilities with the *power grid* has led to numerous vulnerabilities in the cyber-physical system (Sun, Hahn, & Liu, 2018). Organizational leaders should create and check incident management plans to respond to security breaches.

Secure organizations create security framework standards. The framework development process initiated with Executive Order 13636, was released on February 12, 2013 (Schwartz et al., 2018). The development of methods and standards addressed cybersecurity assurance in supply chains to increase societal expectations of sustainable business practices, challenging organizations with a host of emerging risk factors (Zhu, Song, Hazen, Lee, & Cegielski, 2018). Business owners are engaging in technological transformation because of the advancements in cloud computing, analytics, mobile devices, and social media (Sandor, Fulton, Engel-Cox, Peck, & Peterson, 2018). Some organizational owners choose Information Security Management Systems (ISMS) standards to create a set of credentials known as ISO 27001:2013. The ISO management

system standards demonstrate that the organization has the capability to manage information systems successfully.

Cyber Risk Management Framework

A cyber risk management framework also helps organizations protect critical infrastructures. The cyber risk management framework is designed to mitigate common challenges that organizations face when developing analytic models, identifying appropriate annalistic opportunities, and protecting analytic assets (Grossman, 2018). The CISOs need to develop a model to capture the vulnerabilities of cyber capabilities during hazards and propose novel ways to address the vulnerabilities (Zhao, Miers, Green & Mitrani-Reiser, 2018). The NIST MEP Cybersecurity Assessment Tool allows small business owners to self-evaluate the level of cyber risk to their business (Jaruga, Coskun, Johnson, & Kimbrough, 2017). Increasing connectivity, use of digital computation, and off-site data storage provide the potential dramatic improvements in manufacturing productivity, quality, and cost (Hutchins et al., 2015). As threats to information security gain attention in the organization, increasingly interested in asset management gives the organization the ability to defend against cyberattacks.

Cybersecurity breaches make headlines as businesses around the world fall victim to network intrusion and data theft. A comprehensive inventory of all security incidents and breaches, uncovers the security risk organizations face when sharing sensitive information (Yeh, 2018). Security of information is costly; and causes some organizations to invest what is required to protect sensitive information (Luna, Rhine, Myhra, Sullivan, & Kruse, 2016). Some organizations are still hesitant about spending

thousands of dollars to upgrade their security systems and improving data protection policies and practices. Business owners cannot escape the huge financial costs of a data breach, and organizations around the world must prevent business integrity losses as this impacts all industries and processes involving stakeholder private information.

Cyber Impact

Cybercrimes are responsible for the disconnection of computer functions and cause the downfall of many companies. The creation and improvement of technological products and services depend on the exchange of data between people and companies (Olano, 2018). Internet users may be unaware of the different cybercrimes and therefore, may become victims of cyberattacks. Cybercrimes might happen to any business once an entry point, or vulnerability, leads to their information hacking by an unlawful user (Wadhwa, & Arora, 2017). The connectivity between computers through the Internet has made cybercrime a public security issue.

Data breaches have been occurring for as long as businesses kept confidential information and stored private data. Dodel and Mesch (2016) noted cyber-victimization has extensive economic and personal consequences for Internet users as well as negative consequences for economies and the entire cyberinfrastructure (Marti, 2018). The goal of risk managers is to support assertions that the identified risk is manageable to secure and satisfy business owners and stakeholders (Choudhary, 2018). Information security efforts focus mainly on how to improve security and safety technologies (Nishigaki, 2018). Business leaders must work closely to develop appropriate technical controls that minimize the risks that occur in a business.

Business leaders who apply ICT strategies and plans can help cybersecurity professionals to protect organizations. Organizational personnel who use computers can describe their needs for information security and strive to trust in systems that ensure confidentiality, integrity, and availability (Kakucha & Buya, 2018). With the increase in data breaches that occur in the business world, success now hinges on the effectiveness of data protection solutions (Kisekka & Giboney, 2018). Cyber-security systems, which protect networks and computers against cyberattacks, are becoming common due to increasing threats and government regulation (Toch et al., 2018). Cyberattacks affect the way organizations plan and implement information systems.

Cybersecurity

Cybersecurity threats continue to rise and continually take on new forms in response to new protection attempts that flood the cybersecurity market. The definition of cybersecurity is the protection of information from unauthorized access or attacks that are aimed at exploitation (von Solms & van Solms, 2018). Hacking has evolved from a one-person crime of opportunity to an open market of money laundering (Stergiou, Psannis, Kim, & Gupta, 2018). Cybersecurity professionals strive to reduce, filter, and organize large amounts of networks to help reduce the workload of the world's most damaging attacks. Computational models of cognitive processes are employable in cyber security tools, experiments, and simulations to address the organizations and effective decision-making in keeping computational networks secure (Veksler et al., 2018). Cybersecurity tools are designed to categorize and structure network activity to diminish the damage that an attack can cause to the organization.

Cybersecurity is a priority in all businesses. Information is one of the most valuable assets in any market (Aishwarya, Pratiksha, Hule, & Sayli, 2018). According to Paul (2017), SMEs employ 15.7 million people, which is 63% of all private sector jobs. Investment in cybersecurity is critical to small business and medium-size enterprises (Gordon, Loeb, Lucyshyn, & Zhou, 2018). Data breaches rose by a substantial 40% in 2016 (Timms, 2017). Cybersecurity professionals should reduce endpoint complexity and improve internal stakeholder alignment, which would help cybersecurity professionals to pursue more resources.

Cybersecurity Strategies

Cybersecurity threats continue to evolve strategies to mitigate and frustrate cybersecurity professionals. An attacker can launch multiple attacks against a target with a termination strategy indicating that an attacker will stop after observing a number of attacks or when the attacker exhausts resources (Hu, Xu, Xu, & Zhao, 2017). A strategy determines the direction in which an organization needs to move to fulfil the company's mission. As businesses move more, and the business functions of the public network, they must take security measures to ensure that the data cannot be compromised.

Some SMEs encounter multiple cyberattacks daily; many remain undetected. The loss of control over user data has become a very serious challenge, making it difficult to protect privacy, boost innovation, and guarantee data sovereignty (Yin et al., 2018). Since 2017, human-centered cyber research has provided valuable insights into the cognitive and collaborative work within cyber operations but ignored how the genesis, intentions, methods, and outcomes of cyberattacks impact human-related outcomes (Chen, Herrera,

& Hwang, 2018). The SMEs business owners suffer from a lack of access to resources that can increase security with less cost. Companies with inadequate security instrumentation fail to protect their stakeholders, placing legal risks on the business owner.

Remedies. Digital technology tools drive many changes in the business world. Digital technologies have transformed innovation in many industries and sectors (Nambisan, 2018). With many online tools, business leaders have a better insight into customer preferences and form lasting interactions with other businesses. In the contemporary business world, many users expect to engage with businesses through online channels. Using digital technology tools as an online and e-commerce marketing methods benefit small business.

Small and medium businesses are in a necessity for cybersecurity professionals. The SME business leaders should have strategic goals and alternative innovation path in terms of big data and analytics (BDA) (Heikkilä, Bouwman, & Heikkilä, 2018). Big data is a new technology to improve existing business and create new business opportunities. The big data on management control systems influences the way organizations provide empirical evidence regarding control. The big data technology might help businesses address various challenges and provide insights on real-time decision-making. Most literature on big data and analytics focuses on how business leaders can enhance tactical organizational capabilities, but very few studies examine its impact on organizational value (Grover, Chiang, Liang, & Zhang, 2018). The advancement of information technologies changes the way business operates.

Smart power networks in key areas of vulnerability could increase overall cybersecurity. Smart power networks are exposed to an increasing number of cyber-attack events, due to the high integration of information techniques (Liu, Li, Shuai, & Wen, 2017). An effective cybersecurity strategy must work across business security platforms (Cuganesan, Steele, & Hart, 2018). The SMEs can integrate a cyber risk management strategy, comprising obtained cyber insurance into their business to defend themselves from cyberattacks.

Insurance is essential to protecting a business from liability issues related to cyber breaches. The adequacy of insurance for managing cyber risk is to extract cases of cyber losses from an operational risk database and analyze their statistical properties (Biener, Eling, & Wirfs, 2015). Cyber insurance may be a good investment for small businesses that are affected by a cyberattack and do not have the funds to have IT risk audits to prevent a cyber-intrusion.

A performance measurement database must begin by recognizing outcome goals and then using those goals to guide the selection of suitable measures and relate the process and capacity. Once the organization completes the steps, the cybersecurity professional should begin operationalizing performance measures required to access the appropriate data and well-organized resources (Kaban & Legowo, 2018). Cybersecurity professionals should build on existing data systems for purposes of performance measurement and to improve their value for other applications in place.

Business owners are charged with implementing strategies to mitigate the costs of cybercrimes through preventative software and safe online practices for all stakeholders.

Business owners must invest in state-of-the-art technology to make business exchanges safe and confidential for business owners and patrons. Business owners must adapt the growth of organizations' networks to remain competitive. The size and value of the information hacked, damaged, and leaked are increasingly vulnerable for customers and business owners. When business owners build tough systems that deliver interoperable and reliable capabilities, they should establish and adhere to operational cyber styles; this includes the ability to detect different styles and supply innovative solutions that allow conclusive operational benefits.

Privacy and Protection

Maintaining privacy and keeping data secure has always been a very challenging issue for the IT industry. A cyberattack could leave the mass populations vulnerable to unprecedented personal and financial loss. The risk of targeted cyberattackers and the vulnerability posed affects everyone in business and society. Dodel and Mesch (2016) noted cyber-victimization has extensive economic and personal consequences for the Internet users, as well as negative consequences for economies and the cyberinfrastructure. Cybercrimes will impact individuals, businesses, and the economy.

The CISOs professionals are responsible for implementing an information security program, which includes procedures and policies designed to protect initiative infrastructures, systems, and assets from organizations (Georgiou & Lambrinoudakis, 2017). According to Irwin et al. (2018), SMEs constitute most businesses in the United States and the issues impacting their performance is significant for many stakeholders. The open environment of the Internet creates a vital opportunity for businesses to

consider the security of their networks. In addition, the business must ensure that the data is not manageable to someone who is not certified to see it. Unauthorized network access by an external hacker can cause serious damage to copyrighted data, affect the companies' productivity, and hinder the ability to compete.

Privacy protection is more difficult than providing security. Yet, federal law recognizes no difference in the levels of protection expected for physical and electronic data (Casini, 2018). A privacy strategy dictates who should recognize what. The *law* is too often viewed as an impenetrable barrier to the use of administrative data to create and evaluate evidence-based policy (Petrila, 2018). Policies and procedures reinforced by system developments are addressable through the protection of sensitive data recognized by federal laws. Business and governments around the world are committed to sustainable development as a global policy on Internet protections. Cybercriminals use businesses and governments to sell personal and private data to upset critical infrastructures.

Data serve as a vital resource for entry into new markets, strategic partnerships play a critical role in capturing the value created through the exploitation of data resources (Mamonov, & Triantoro, 2018). With the rapid growth in technology, cloud computing has become increasingly popular among individual users and businesses around the world (Changchit & Chuchuen, 2018). Organizations can capture value from new technology by incorporating the technology in their current businesses.

Communication privacy management (CPM) provides a framework for understanding how small and medium business should maintain privacy parameters.

When a cybersecurity professional discloses information to a third party, the third party becomes a co-owner of all the information and in some cases, that co-owner could disclose personal information to a hacker. All cybersecurity professionals should have a degree of control over the information. Connectivity and information flow represent the two key enabling factors for a successful operation of the digital world (West, 2018). Connectivity within the business process is not new.

In summary, cybercrime poses an increased risk to businesses, customers, global entities, consumers, families, and society by infiltrating and stealing vital and confidential information, for the purpose of personal and illegal gain (Hu et al. 2017). The costs to businesses are far-reaching, but the personal costs, including the loss of trust in secured interactions and transactions is detrimental to business security and reliance on *secure* exchanges. The insidious nature of theft against the public, and the methods used to infiltrate accounts and personal information is unfathomable. The alarming extent of the problem highlights concerns about using the Internet at all as the Internet may pose extreme risks to individuals, particularly those exchanging money for merchandise online. Hackers face limited challenges in accessing personal account information, using personal accounts for illegitimate purposes, and creating significant debt for unsuspecting Internet users.

Business owners are responsible for the safe delegation of services to all stakeholders who use the business online services. There is an expectation upon businesses that, with the private customer information stored within the business' database, that the information is secure and inaccessible to others. This remains an

assumption, and reports of entire systems under siege remains commonplace within the business environment. Business owners must become knowledgeable about the risks of cyberattacks directed at their company, and work to prevent cybercrime. This may involve working with employees to promote safe Internet practices, ensuring encrypted and secure transactions as a standard business practice, and most importantly, protecting the integrity of the company through the protection of consumer data, business unethical practices, and business reputation (Yeh, 2018). While companies provide some solutions to these issues, a thorough exploration into what strategies CISOs of high-technology companies use to protect their businesses from cyberattacks may aid in protecting the growing number of businesses who may not have strategies, or the capabilities to prevent cyberattacks.

Transition

Section 1 contained an introduction to the study regarding what operational strategies CISOs of small high-technology companies use to protect their businesses from cyberattacks. Section 1 included the background of the problem, problem statement, purpose statement, nature of the study, research question, interview question, conceptual framework, operational definition, and significance of the study. In addition, section 1 included a discussion of the assumptions, limitations, and delimitations of the study. The conclusion of section 1 included a literature review of the professional and academic literature. Section 2 included the discussion of the role of the researcher, participants of the study, research method, and design, population and sampling, ethical consideration in the research, data collection, organization techniques, and data analysis technique. In

Section 3, I included an overview of the study, presentation of the findings, the application to professional practice, the implications for social change, recommendations for action, recommendations for further research, reflections of my experience conducting this study, and a research conclusion of this study.

Section 2: The Project

In Section 1, I provided a detailed review of the literature related to the central research question. In Section 2, I expand on the methods and techniques I used to conduct the research. I include a discussion of ethical requirements and strategies to ensure the reliability and validity of the research. In Section 3, I will provide the findings of the research, implications for social change, and recommendations for further research.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies CISOs of high-technology companies used to protect their businesses from cyberattacks. The target population consisted of business leaders from three small businesses operating in Florida who successfully protected their business from cyberattacks. Cybersecurity managers were appropriate participants for this study due to their knowledge and expertise in preventing cyberattacks. CISOs and other business leaders could use findings from this study to better provide customers with a safe and secure environment for conducting electronic transactions.

Role of the Researcher

My role as a qualitative researcher involved collecting and analyzing data from the research participants, reviewing available documentation, and reviewing social media sites to answer the central research question. I was the interviewer and primary data collection instrument for this study. All participants had the capability to choose whether or not they wanted to participate in this study. A qualitative researcher becomes well-versed in strategies to minimize risk to participants. Bartlam et al. (2018) noted

participants act independently of the researcher. Additionally, researchers and participants can be ethically challenging for business leaders, due to the personal involvement in different stages of the study (Sanjari, Bahramnezhad, Fomani, Shoghi, & Cheraghi, 2014). I collected data until no new information was available to achieve data saturation.

My role as a researcher involved adhering to the research ethics and Belmont research protocol. The Belmont Report summarizes ethical principles and guidelines for research involving human subjects (Pearce, Ensafi, Li, Feamster, & Paxson, 2018). According to the Belmont Report protocol, a researcher's responsibility is to provide beneficence, provide respect-for-persons, and justice to each participant (Ross, Iguchi, & Panicker, 2018). Palmas (2018) noted the Belmont Report principles as an ethical frame of reference. Respect for participants ensures that all participants have space to make independent decisions (Reid et al., 2018). Justice is the concept of equal treatment for everyone (Leiber, Beaudry-Cry, Peck, & Mack, 2018). I abided by the Belmont Report by respecting respondents, minimizing risks, maximizing study benefits, and avoiding impartial selection of participants.

For this qualitative multiple case study, I collected data from managers working in information technology. Interviews were my main mode of data collection (see Yin, 2014). I also reviewed company websites and social media pages. For the interviews, I used an interview protocol (Appendix A). An interview protocol contains the interview questions and step-by-step guidance that I used consistently to ensure the interview

process was reliable. An interview protocol includes having a ready set of interview questions and using a script to ensure the capture of rich thick data from each participant.

Participants

The sample for this study included individuals working in information technology whose Florida businesses were impacted by cyberattacks. I explored the strategies those businesses use to prevent future attacks. I initiated the data collection process after receiving the approval from the Walden University's IRB, and I used purposeful sampling to recruit participants. In most case studies, coordinating resources and using a small number of expert participants is critical (Yang et al., 2018). The participants in this study are individuals operating small businesses. The study included two high-technology companies operating in Florida that have successfully protected businesses from cyber-attacks. An excellent case study includes collecting interviews from multiple businesses and analyzing the connections across those businesses. To meet the criteria for this study, participants had to work within a business impacted by a cyberattack, were equipped to respond successfully to remain operable. All signed a concent form before I began their interviews.

To recruit participants, I connected with them through LinkedIn and I emailed the informed consent form to each participant. The consent form also served as the invitation letter, and a reply with an "I consent" indicated agreement to participate in the study. The interview participants where individuals working for small and medium-sized businesses who protected businesses from cyberattacks.

Research Method and Design

Research Method

The three types of research methods are qualitative, quantitative, and mixed methods. The quantitative method is appropriate for evaluating hypotheses with inferential statistics (Spicker, 2018). The quantitative method was not appropriate for this study because it requires a hypothesis test. Mixed method was not appropriate because it requires examining relationships or differences between variables, which was not required for this study. The mixed methods approach is useful when combing the participants' experience and empirical data to determine the relationship and identify the variables (Yin, 2014). Qualitative research method examines strengths and limitations while discussing important contributions to the study (Latunde, 2017). A qualitative method was the best choice for this study because qualitative descriptions are important to expose dynamic processes (Matt, Gaunand, Joly, & Colinet, 2017). I used it to explore operational strategies CISOs of high-technology companies used to protect their businesses from cyberattacks. With this design, I captured information through interviews, a review of available documentation, and a review of social media sites.

Research Design

Multiple case study was the most appropriate research design because the purpose of my doctoral study was to explore operational strategies CISOs of high-technology companies used to protect their businesses from cyberattacks. Case study research is a useful approach for exploring contemporary phenomenon within real-life settings. Yin (2014) noted that a case study researcher investigates a phenomenon within a specific

context to address the research questions. A phenomenological design is used to maximize the depth of information collected (Burns et al., 2018). A phenomenological design was not appropriate because I wanted to explore beyond lived experiences to also capture perspectives, and any evidence found in documentation or social media sites, to triangulate the research. A narrative researcher explores aspects of an entire lifetime to explain phenomenon. The life stories of the participants in this study had no relevance in the decision making processes participants used to protect their companies from cyberattacks; therefore, the narrative design was not appropriate for this study. The case study provided the best opportunity to gather data from various sources and was the best approach to answer the central business question.

Population and Sampling

The population for this qualitative multiple case study consisted of CISOs from high-technology companies operating in Florida who successfully protected businesses from cyberattacks. The participants worked in the information technology field from a specific sector and geographic area. In this study, I used a snowball sampling to recruit businesses owners whose businesses were affected by cyberattacks. Robinson (2014) developed an approach to sampling in qualitative research that includes (a) defining the sample universe, (b) deciding on the sample size, (c) devising the sampling strategy, and (d) sourcing the sample. Purposive sampling ensured I recruited those who would share expertise to strengthen the study and assurance that the participants I selected were experts in the cybersecurity field. I used a purposive sampling method to identify interviewees who met the established criteria for the study. The study included a

purposeful selection of three small business owners. Purposive sampling allows a researcher to complete projects on time using data collected from businesses (Mohr & Metcalf, 2018). Data saturation is when no new data or information is needed (Moser & Korstjens, 2018). This purposive sample was sufficient to reach data saturation.

Ethical Research

As a researcher, my role was to protect the integrity of the research, beginning with protecting the confidentiality of participants and performing the investigation in a respectful and cautious manner. My first task prior to conducting research was to complete the Protecting Human Subject Research Participants training by the National Institute of Health. Once I gained IRB approval to conduct research, I sought to ensure all participation in the research was voluntary and that any request to withdraw from the study was supported. I also ensured that, prior to interviews, I received participant consent and informed participants of all rights related to their involvement in the study. Research must be conducted in a manner that poses the least amount of harm to participants (Ko, Ma, Bartnik, Haney, & Kang, 2018).

Informed consent is critical in research with participants (Moore, McArthur, & Noble-Carr, 2018). Although no participants withdrew, participants were allowed to withdraw from the study at any time before and after the interview. I used acronyms to protect the personal identity of the participants according to the order of the interview where the first participant is PA1, the second is PA2, and the third participant is PA3. To comply with Walden University's standards, I will secure all interview results for at least 5 years and then destroy them. A letter outlining the research scope and offering

introduction was provided to participants. It included details of the study, the requirements for participation, and acknowledgement that they could withdraw from the study at any time. The participants received no incentive for their involvement in the study. However, each participant will receive a final approved copy of the study. Walden University's IRB approval number for this study is 01-24-19-0634075.

Data Collection Instruments

In this qualitative study, I was the primary data collection instrument. I collected data from CISOs operating in Florida. The case study interview protocol includes the interview questions, comprises a description of the organization's procedures and general rules guiding the research (Yin, 2014). Yin (2014) argued that the interview protocol helps increase the reliability of case study research. Yin (2014) described that the investigator in a case study must (a) ask important questions, (b) be a good listener, (c) show flexibility, (d) have a firm grasp of the subject topic, and (e) avoid any bias. Renz, Carrington, and Badger (2018) described involving the collection of data through extensive interviews, note taking, and tape recording. Member checking and thematic analysis adds validity to the study (Comley-White & Potterton, 2018). I used member checking to ensure the accuracy of the data collected, data saturation, and appropriate interpretation of the data.

Data Collection Technique

Data collection techniques depend on the research design approach that will most appropriately answer the research question (Yin, 2014). A qualitative multiple case study design guided the research process and was the best approach in gaining a good

understanding of the phenomenon. Interviewing participants, reviewing accessible documentation, and physical artifacts are the most common forms of valuable data in a case study (O Nyumba, Wilson, Derrick, & Mukherjee, 2018).

Before I conducted the interviews, the participants received a consent form. I explained the details of the consent form. The consent form included an explanation of the study, an explanation of what is required by participants including the right to withdraw at any time. I provided a space on the consent form for participants to consent or decline the invitation to participate in the study, and informed those who participate, they will receive a courtesy summary of findings following the research. Once consent forms were signed and returned, interviews were scheduled.

An interview is a technique for collecting data in which the researcher asks open-ended questions (Smith, & McGannon, 2018). I used semistructured, face-to-face, open-ended questions in this study. Using a semistructured interview technique provides an opportunity for flexibility in the interview process, and to probe to gain rich, thick data, to draw insightful conclusions (Nyström, Karltun, Keller, & Gäre, 2018). Semistructured interviews could yield a broad range of perspectives, and cumulatively, these add texture to the data collection process. Face-to-face interviews help build trust between the researcher and the participant (Ciocănel, et al., 2018). The interview protocol used to guide the interviews is provided in Appendix A.

Each interview took approximately 30 minutes with a brief introduction. During the interviews, I solicited answers from the participants, reflecting the experiences and perspectives of cybersecurity professionals. The script included an introduction to the

interviewer, the process of the study, information about the study, and the interview questions. I encouraged the participants to provide the names of additional potential participants who met the criteria. The interview ended with a statement thanking the participants for their participation. After the initial interview, I engaged participants in a follow up member checking session to verify the accuracy of their statements and add any new information to their previous statements. Following the member checking, I transcribed the interview material and prepared the data for analysis.

Data Organization Technique

To protect the integrity of the study, I organized the data for security and quick-retrieval purposes. I emailed the consent form to every participant once the participants agreed to participate in the study. I secured the confidential information of the participant by coding with letters and numbers. I kept all the research data such as recorded interviews in one file or in a journal notebook and after the interview. Data collected from participants is saved in a Google drive and data entry software Excel. Each participant has a dedicated section in the Google drive and data entry software Excel. The section included a copy of the consent form, a copy of the transcribed interview data and all notes the researcher collected during the course of interviews. A copy of all collected data for the study is stored on an encrypted USB drive for at least 5 years. All stored data have a password protection for confidentiality.

Data Analysis

Data analysis involves drawing key information and strategies from the interview data, information gained from the organization, social media sources, the conceptual

framework, and the literature, exposing a number of themes that explained the central research question. I analyzed the data once the collection of data reached saturation and all information has received member checking and transcription. Qualitative research enables richer accounts but inevitably includes coder bias and subjective interpretations (Cabrera & Reiner, 2018); however, the value gained from face to face interviews far outweighs risks of bias that were duly noted and mitigated throughout the research process. Data analysis refers to the assessment of gathered information from three sources (a) notes, (b) interview responses, and (c) additional source materials collected from the organization (Kern, 2018). Multiple sources of data helped to ground the reliability of the research. I used methodological triangulation to strengthen the reliability and validity of the study by conducting interviews, reviewing organizational offerings, and review social media sites. Methodological triangulation is the exploration of additional materials to form a conclusion (Rodgers et al., 2018). Researchers use triangulation to enhance the confidence of a study by comparing, contrasting, and confirming information and through checking the integrity of their inferences (Yin, 2014). Methodological triangulation adds validity to the research study (Yin, 2014).

The data analysis process included the use of software called NVivo, which is a computer-assisted qualitative data analysis software (CAQDAS) for data collection. The NViVo software provided features to automate and analyze data generated through a selection of inputs. The NVivo software enables the researcher to code the data and draw connections between codes to identify themes (Pokorny et al., 2018). After transcribing the interviews, I categorized and coded key ideas in the responses, and through NVivo

software, I established themes from the interview data. I then incorporated the additional source data collected, compared the findings to the conceptual framework and literature reviewed, and established key themes representing the findings of the study. The data I collected allowed me to answer my central research question of how small and medium-sized businesses companies lack operational strategies to protect their businesses from cyberattacks.

Reliability and Validity

Reliability

Reliable research is consistent in protocol, delivery, and outcomes (Leung, 2015). For a qualitative case study, reliability means that the study is repeatable and will provide similar results by following the same defined processes (Yin, 2014). Carefully asking direct questions related to the central research question, recording responses, and then ensuring the accuracy of the responses through member checking, all help to create confidence in the procedures and findings of the study (Grossoehme, 2014). Using an interview protocol ensure that the researcher applies the same techniques to each interview to prevent bias and inconsistencies in the interview process. Therefore, I used an interview protocol and ensured each question was relevant to the central research question.

A rigorous approach to qualitative research yields the best representation of participant experiences and perspectives (El Hussein, Jakubec, & Osuji, 2015). Marshall and Rossman (2016) added triangulation also helps to strengthen qualitative inquiry. Carter, Bryant-Lukosius, DiCenso, Blythe, and Neville (2014) indicated that triangulation

is a means of drawing various sources of related information together to explain phenomenon. I interviewed the participants, reviewed company documents, and social media sites, as a means of triangulating the study.

Validity

A valid study requires the use of appropriate methods and analysis processes to establish sound results (Leung, 2015). Marshall and Rossman (2016) argued that methodological triangulation of data from multiple sources, member checking, and peer debriefing improves the validity of qualitative research. Carter et al. (2014) discussed the importance of triangulation in qualitative research to ensure that more than one sources leads to any conclusions about a phenomenon. Member checking adds to research validity by ensuring that the interview data collected is interpreted accurately. Participants review their contribution to the study, update any misinformation, and may provide additional evidence to strengthen their arguments (Andraski, Chandler, Powell, Humes, & Wakefield, 2014). I used both methodological triangulation and member checking to ensure the validity of the study.

Trustworthiness in qualitative research builds confidence and credibility in the study (El Hussein et al., 2015). Trustworthiness incorporates transferability, confirmability, and credibility into the research process. Transferability results from a researcher applying findings from one study to another situation and presuming the study would have similar results.

Kihn and Ihantola (2015) added that the Researcher achieves confirmability when the research findings are easily transmitted and understood. Data saturation in

interviewing requires that the researcher continue to ask interview questions until the study reaches as point where the addition of new data adds no new information, and at that point the interviews stop (Fusch & Ness, 2015). Creating an audit trail is aided by the use of NVivo software, adding credence to the research processes (Houghton et al., 2013). Detailing each step within the interview protocol and audit trail help to validate the study further (Morgan, 2016). Member checking further adds trustworthiness to qualitative research (Kornbluh, 2015). By using the interview protocol (Appendix A), saturation, methodological triangulation, and member checking, I assured the trustworthiness and validity of the study.

Transition and Summary

In Section 2, I provided a restatement of the purpose of the study, the role of the researcher, participants and population, the research design, and methods. In addition, I also discuss the data collection instruments, techniques, and data analysis. The most appropriate research method and design were the qualitative multiple case study to explore operational strategies some CISOs of small high-technology companies use to protect their businesses from cyberattacks. Section 3 includes details on the findings of the research, implications for social change, and recommendations for further research.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the operational strategies CISOs of high-technology companies use to protect their businesses from cyberattacks. In this section, I present my findings and discuss the themes identified. I also discuss applications to professional practice and implications for social change, and provide recommendations for action and further research, personal reflections, and conclusions. The participants provided me with interview data that I used to address the research questions, in conjunction with organizational documentation, social media forums, and the literature review. Cybersecurity professionals highlighted the need for skills in the area of communication, gaining knowledge of current cyberattacks, and risk to the business.

Presentation of the Findings

The central research question for the study was: What operational strategies do CISOs of high-technology companies use to protect their businesses from cyberattacks? I asked three cybersecurity business leaders a series of questions on strategies to prevent cyberattacks. During the data analysis process, I identified four main themes: (a) effective leadership, (b) cybersecurity awareness, (c) reliance on third-party vendors, and (d) cybersecurity training. The conceptual framework guiding the study was organizational learning theory. In Table 1, I provide a summary of participants' demographic information of the. The three participants had over 26 years of combined experience working in the cybersecurity field with small and medium-sized businesses.

Table 1

Cybersecurity Professionals' Demographic Information

Characteristics	Case 1	Case 2	Case 3
Code name	PA1	PA2	PA3
Age	36	45	55
Highest level of education	Bachelor's degree	Master's degree	Master's degree
Length in current field	6 years	9 years	11 years
Years of experience as a business leader	10 years	5 years	15 years

Theme 1: Effective Leadership

Leadership was the first theme that I identified through data analysis. Leadership in the organization was the first factor that participants stressed as important in engaging cybersecurity professionals in their leadership teams. The three participants agreed that leadership in their organizations is motivating and transformational. In the business world, leaders should play a strong role in professional life since leadership has a great impact and influence on individuals (Moore et al., 2019). Effective leaders lead with a vision, and effective leadership motivates followers to perform their best when executing the organization's policies after a cyberattack. Laureani and Antony (2019) explained that effective leadership involves the right leadership style to attain the appropriate level of motivation and vision after an attack on a business. All the participants agreed that the business leader should create and communicate an inspiring vision for everyone working in the workplace. The participants agreed that the vision sets the purpose of the business.

The effective leadership theme confirms the findings of Frieder, Wang, and Oh (2018) that leader personality traits impact employee job performance especially when the manager emphasizes the meaningfulness of employees' work. The theme also resounded with the findings of Ashford et al. (2018) that showed the role of optimism and foresight in developing a robust and inspiring vision for the business' future. Ashord et al. (2018) indicated cybersecurity professional needs and use of resources are on the rise in most organizations, and this development requires key leadership attributes to advance the company competitively. Participant 1 indicated, "A growing organization develops its security program, to guide the company in times of crisis and change, and keep it on track." Participant 2 indicated, "An effective leader must be a motivator and team builder to be able to facilitate different roles on how to be an effective leader." While Participant 3 indicated stated, "Different leaders carry out different leadership responsibilities." According to Nieuwboer et al. (2019), effective leaders dwell on the ability to lead others and for that reason, a leader must adopt effective characteristics to ensure their style of leadership is effective. The effective leader portrays maturity and skills and the capacity to provide direction through constant change.

All participants noted that effective leaders can help employees advance with the influence of a higher level of motivation. Participant 1 indicated, "Leaders can help followers experience the same passion and motivation to fulfill the organization vision." Participant 2 indicated, "Hiring effective leader experts can help organizations find a cost-effective strategy to introduce best practices in the business." And Participant 3 indicated, "Effective leaders help others develop into leaders by replying to individual

needs and by aligning the organization goals." Some capabilities may come naturally to business leaders, while others are developed and strengthened over time. Business leaders are faced with encounters such as satisfying employee morale, budget cuts, and reorganization. Furthermore, business leaders are also responsible for satisfying employee morale and being a visionary and a role model within their respective agencies (Kopaneva, 2019). However, not every effective leader is an ethical leader. Bastian (2019) specified one key difference between an ethical leader and an unethical leader is the means used to motivate others and achieve goals. All participants agreed that to be an effective leader is to lead toward a designated goal. An effective leader is able to advance an organization and its stakeholders to new goals and outcomes. Evidence for this theme emerged primarily from participant interviews, and was supported by the literature and conceptual framework.

Theme 2: Cybersecurity Awareness

The most important factor in cybersecurity awareness is to make people aware of their responsibilities and roles in information technology. Cybersecurity awareness is one of the resources that businesses depend upon. Cybersecurity awareness prevents information and business compromise. Business leaders should be aware of the risk in the industry and inspire growing awareness of information security in their organizations. Cybersecurity awareness involves knowing how to protect business information and how to take reasonable steps for preventing data breaches.

The second theme that emerged through the research was the need for cybersecurity awareness. The goal of cybersecurity awareness is to increase

organizational knowledge and prevention of cyberattacks and apply best practices. All the study participants indicated that cybersecurity programs should apply to everyone working in the business. Some businesses are conducting awareness training about security vulnerabilities in the businesses because cybersecurity training ensures everyone working in the IT department is aware of the risks and responsibilities of protecting information technology assets (Bhardwaj & Goundar, 2019). Cybersecurity awareness is increasingly relevant to all business operations to ensure the protection of company assets.

Triangulation of interview data and available documentation provided many revelations related to cybersecurity awareness. The review of Participant 1 indicated security documents showed a "comprehensive card data security clarification," which contains electronic chip technology to authentic clients' cards, and end-to-end encryption and tokenization services to safeguard consumers' information. Participant 1 indicated, "We have a processing credit and debit payments that helps protect against new and evolving fraud threats by realizing EMV chip technology and encryption security technologies in conjunction." Participant 2 indicated security plan showed "the impact of tokenization on Payment Card Industry (PCI) agreement." Small and medium-sized business leaders suggested not only awareness, but also the need for cybersecurity protection by creating and applying a written security policy. Participant 2 indicated, "The business tie in the reasons that show changes in digital habits to protect ourselves online which includes phishing scams and social engineering." Participant 3 indicated, "Cybersecurity awareness is the not only the business concern but it also concerns

insufficient awareness." In addition, Participant 3 indicated, the business has an urgency and adaptably to new opportunities as they arise.

Cybersecurity awareness in information systems training has become one of the most important necessities in an organization. Lykou, Anagnostopulou, and Gritzalis (2019) noted constant moving and technologically fragile safe communication systems are required to ensure business sustainability and profitability. Participant 2 indicated, "In order to decrease the number and extend in security breaches then training is fundamental."

Effective cybersecurity awareness programs can improve the information assurance of an organization. Information security incorporates organizational aspects, legal aspects, and presentations of best practices in security technologies. Participant 1 indicated, "User awareness signifies a significant challenge in the security field, with the human factor finally being the element that is manipulated in a range of attack settings." An information security awareness program is a vital component of any organizations policy. In the competitive market, cybersecurity attacks result in loss of income, loss of customer trust, and liability issues. Therefore, information should be safeguarded and protected.

Participant 1 indicated, "Various organizations use expedient information security awareness tools established by some of the international information security companies, whereas some organizations make their own awareness tools according to the needs of the organization." Participant 2 indicated, "Information security awareness is about guaranteeing that all personnel is aware of the rules and regulations regarding securing

the information within the business. Information security awareness should, therefore; form an important part of any establishments' overall information security management plan." Participant 3 indicated stated, "Sending out a report monthly on all activities can reinforce learning and the value of the business."

Cyber attacks is reality and can cause a lot of damage if business leaders do not target a critical infrastructure. Hackers seek to coerce users into allowing them access to a digital resource before they try to hack their way in. Therefore, due to the quickly changing environment, cybersecurity awareness training cannot involve a one-shot program. In order to safeguard the network security of a business, cybersecurity teaching must be repetitive, efficient, and repeatedly tested.

Theme 3: Reliance on Third-Party Vendors

The third major theme to emerge during data analysis of archival documents and participant interviews was the use of cybersecurity policy and the business leaders' documents that provide details on defending organizations and their assets. I found the more the business relies on technology to collect data, store or manage information, the more vulnerable the business becomes too severe security breaches. Human errors, hacker attacks, and system malfunctions could cost the business financial damage and can jeopardize the business reputation. My analysis specified the requirements cybersecurity professionals use to maintain a network system. An important requirement of any information management system is to guard data and resources against breaches, while at the same time safeguarding data access to genuine users.

Participant 1 indicated, “I have experience in managing highly secure organizations of major enterprises by closely integrating security and operations and the necessity small and medium-sized business owners used to launch cybersecurity policies and efficiently implement cybersecurity techniques to protect their businesses from cyberattacks.” One of the challenges of responding to a cyberattack was the nonexistence of consistent security policies and procedures disclosures a business to unforeseen threats. The participant noted that dealing with systems handling data are delegated to track its flow to comply with data protection regulations.

Participant 2 indicated “The goal of the company is to capture the magnificent breadth of valid policies”. My study required participants to analysis also specified the requirement for cybersecurity professionals and business leaders to implement cybersecurity procedures to protect their businesses from cyberattacks. The participant also noted to reduce expenses resulting from hackers, everyone in the business needs to communicate, implement, and sustain security policies.

Participant 3 indicated stated “A common enterprise-wide approach has not yet been implemented, however; for some business, the responsibility for cybersecurity has entrusted almost entirely on the chief information security officer.” The cybersecurity professionals believe that the teams should be led by the business leaders with an organized strategy. One of the tasks to teamwork has been the official business environment of the cybersecurity and a surviving condition that need be addressed when a business entrench the risk thinking and task in cybersecurity strategy.

Business leaders must take a proactive approach to protect their data by establishing cybersecurity plans. As organizations expand their operational processes to their cyber infrastructure, effective cybersecurity is the key to an organization ability to protect their assets. Participant 2 indicated "Working in the cybersecurity field is important because it is not just about protecting the company and the company assets, it is also about protecting the company reputation, property, and customers". The business owner believes the investment can be complex technical solutions, which mean that they are well protected from cyberattacks. Participant 2 indicated believed that it is part of an operational defense.

Business leaders facing threats must safeguard that they have a unified approach to cybersecurity tailored to their particular business and risk profile. According to Participant 1 indicated, "It is not only about addressing the technical aspects of their defense, but it is also about the organizational elements". Participant 1 indicated had an in-depth understanding of the threat and risk-based approach to identify how it affects the individuals in the business. An effective cybersecurity strategy must work across a business security measure. Participant 2 indicated, "Capability in a range of key disciplines with the ability to work across organizational functions to strengthen an integrated cybersecurity strategy." All organizations need to plan for a successful cyberattack and it is also essential to ensure they have the ability and resources to rapidly detect and isolate any problems that occur, control the level of the investigation and respond immediately to any inquiries, and maintain business continuity. Participant 3 indicated, "Risk oversight of cybersecurity practices and the business always ensure the

strategy to protect their assets." Lastly, it is important for security objectives are to ensure continuous security measures. The business must review all the risks in all departments and mitigate the most important risks by applying defense and responding to a crisis in a prioritized way.

Theme 4: Cybersecurity Training

The business leader established a cross-training on various product lines and career expansion for the talented remaining employees. The cross-training prepared individuals for transferring to a different product line or department to keep busy and engaged. The business leader is providing information and opportunity for achieving their career desires through organization-specific preparation and guarantees that they are part of the business because it is important to the employees. Loon (2019) emphasized that human capital development is accepting individual foundational theories of socio-economic development. Participant 1 indicated "Some employees are worried that they don't have the understanding and skills needed to take on new tasks, or expand on the business. While others are worried about having the time and energy necessary to step up to the larger task. Participant 2 explained "It is hard to find talented cybersecurity professionals due to the money the organization needs to spend and having the time to train that individual." Participant 3 added "The people who report to you worry for various reasons."

Participant 1 and Participant 2 indicated to invest in personal training and improvement to develop employability while business leaders participate in employee-specific training to improve organizations' efficiency. Participant 3 indicated "Personal

training improved the business efficiency and safety." In my examination of the participating businesses' websites, I recognized reports such as "we invest in the learning and development of our employees to increase competency" and "we invite, retain, and improve our people." All the participants emphasized that there is a shortage of talented cybersecurity professionals willing to work with small and medium-sized businesses.

Supply chain finance, as the core driving force for supply chain development, plays a vital role in resolving any financing difficulties that exist in many SMEs in the upstream and downstream of the supply chain (Liang et al., 2018). Employee productivity is essential to any business. Business leaders found when teams are able to make significant gains and developments in a short amount of time, it can have a massive impression on the bottom-line (Liang et al., 2018). The more well-organized your employees are, the more positive you'll be as a business. However, most agree that employee productivity is important, but there's a lot of misinformation about it. There are countless business leaders doling out information on production. Occasionally, this information could be good and bad. While it's not supported in truth. Therefore, this theme supports the human capital theory in that the savings in training and education lead to improved benefit for both the organization and the people business leader employed. To assess employee production, as well as progress operational programs for improvements, business leaders need to engage in research, which is one of the reasons one business leader gathered a comprehensive list of employee productivity measurements. Therefore, is most important to encourage the people who report to you of their importance to you and the organization. Business leaders need to talk with each

person independently to let them know why and how they are valued to the organization, highlighting their support to the overall functioning of the operation. For some, it will be exciting and career-expanding.

Applications to Professional Practice

The findings of this study could prove valuable to current and future leaders in the cybersecurity field. Study findings may also help business leaders and cybersecurity professionals reduce costs when responding to cyberattacks on businesses. The cost of responding to cyberattacks has risen because of the need for cybersecurity professionals needed in the market and due to the increased number of cyberattacks affecting business operations (Abhishta, van Rijswijk-Deij, & Nieuwenhuis, 2019). Therefore, small and medium-sized business owners can improve their business performance and best practices to protect their businesses from cyberattacks. The study findings include four themes: (a) effective leadership (b) cybersecurity awareness, (c) reliance on third-party vendors, and (d) cybersecurity training. A tactical plan is serious because an awareness plan provides the foundation to secure a business and how business could prevent cyberattacks. Furthermore, the findings and conclusions can help small and medium-sized business leaders mitigate against the problems arising from regulations. Access to information about procedures should be available to small and medium-sized business at minimum cost. Policymakers must ensure that the compliance procedures associated with new technologies are not pointlessly overpriced, difficult, or extensive. In general, small and medium-sized enterprises account for over 95% of businesses and 60% to 70% of employment and generate a large share of new jobs (Alcalde-Heras, Iturrioz-Landart, &

Aragon-Amonarriz, 2019). Business leaders have specific strengths and weaknesses that require special policy and procedure responses. As businesses see new technologies, the reputation of economies of measure in many activities firms enhanced and the potential contribution of smaller firms is greater. However, many of the traditional difficulties facing small and medium-sized enterprises include the lack of financing, problems in developing technology, controlled decision-making abilities, low efficiency, technology-driven environment, and the business becomes more acute in globalization. Current and future business leaders could adopt approaches to cybersecurity that will require much more engagement from the cybersecurity professional to protect critical business information without constraining innovation and growth.

Implications for Positive Social Change

The implications for social change from this research include the potential impact of successful cybersecurity strategies for small and medium-sized business owners to protect their business from future cyberattacks. The biggest issue that small and medium-sized businesses are facing is defending themselves from potential cyberattacks and some businesses had to pay cybercriminals even up to $1 million in a single attack, while others have incurred losses in hundreds of millions of dollars (Zimba, & Chishimba, 2019). In organizational learning theory, both single and double-loop learning deal especially with the idea of the organization as whole learning and adjusting its behavior. Organizational learning theories are included in this study since they deal with both policies and employee behavior. The findings of the study draw attention to specific

approaches needed to strengthen businesses and optimizing the use of the Internet to ensure businesses retain a competitive edge while diligently preventing cyberattacks.

Training employees and giving them career growth chances is one guaranteed way to show them that the business can invest in their future? It will influence individuals to keep employed strenuously and be improve at their jobs. These opportunities are equally useful since training opportunities help grow the company while at the same time they further employee knowledge and skills. Small and medium-sized businesses can be characterized as *advanced***,** of which some 5 percent are *technology-based*. Advancing small and medium-sized business tend to be *market-driven* rather than research-driven, and speedier in responding to new opportunities than large businesses. Business leaders play an important role in groundbreaking and increasing new markets. Programs for educating the diffusion of technology have removed from a supply focus to educating the *capacity of small and medium-sized enterprises to engage technology*. The findings from the study could contribute to social change by investing in other small and medium-sized enterprises, new entrepreneurs, and academic establishments with successful strategies and incomes to effect changes within the community.

Recommendations for Action

The purpose of this qualitative multiple case study was to explore what operational strategies CISOs of high-technology companies use to protect their businesses from cyberattacks. Based on my findings of this study, I recommend several actions that the current and future cybersecurity professionals to strengthen their cybersecurity capabilities for the future. First, cybersecurity professionals need to properly develop ways to identify and prioritize IT security risks and improve mitigation strategies which hundreds of millions of dollars have been devoted to implementing these

strategies. Second, desktop environments are more vulnerable than they were even five years ago, as USB ports have been restricted and Webmail services are blocked in some businesses. Third, robust technologies and enterprises have been put in place to address attacks on the perimeter. Therefore, business leaders interviews strengthened changes in how enterprises use technology have concurrently made corporate environments tougher to protect while snowballing the importance of protecting them. Recommendations (a) mitigating actions should flow logically from the conclusions and contain steps to useful action, (b) state who needs to pay attention to the results, and (c) indicate how the results might be disseminated via literature conferences, training, and so on. Business leaders need to expand their range of potential candidates to seek smart, encouraged and enthusiastic individuals who work well as part of a team. One business leader felt that because they may not have the degrees, certificates or prior experience a company might hope for doesn't mean they won't be an excellent fit. I intend to publish the study and take advantage of opportunities to share with business leaders in the cybersecurity field, colleges and university, and business forums where business leaders discuss strategies to avoid the unsuccessful concerns of a major cybersecurity breach.

Recommendations for Further Research

I conducted a qualitative multiple case study on the strategies used by business cybersecurity professionals. The population for the study consisted of two small and medium-sized businesses owners use to protect and defend their business from cyber-attacks. The study is also limited to one geographic location. Thus, to generalize the findings, future researchers can decide on different location such as researching different

organizations impacted by cybersecurity or businesses around the countries. Furthermore, future researchers should consider doing the study in a different industry such as nonprofit organization, small and medium-sized businesses, government agencies, and high-technology companies. Additionally, future researchers can use a mixed research method to report on changes in cyberattack frequency, geographic location, preparedness and mitigation strategies across a vast area. The findings of such a study, paired with evidence from qualitative interviews and related evidence, will inform policymakers and ensure a viable and aggressive response to protect businesses, consumers, and society from the insidious impact of cyberattacks. I would recommend future researchers to consider allocating additional time to obtain viable research to determine the effectiveness of the cybersecurity field and make recommendations to address gaps in security that may impact broad domains, in an era of ease of access and clandestine actions to undermine the core economic structures of society.

Reflections

Completing the doctoral study process has been a rewarding experience since I did not have any knowledge in the cybersecurity field. I learned valuable information about cybersecurity in small business, what methods cybersecurity professionals use to prevent cyberattacks, and about conducting qualitative research. The results of the study helped me to understand the importance of protecting a business and why it is important to hire cybersecurity professionals and to understand the difficulties of conducting qualitative research. This qualitative case study explored successful strategies used by business cybersecurity professionals. The results of the study helped me to understand the

difficulties of conducting qualitative research. Finding participants for a limited case study can be very challenging. The problem results from companies not securing their networks and small businesses need cybersecurity professionals in place. There are a limited number of companies with cybersecurity professionals in Florida.

The data collection and analysis was sensational and fulfilling. I had a few difficulties finding participants due to their busy schedules and wanting to ensure the proper information to give to me due to sensitive information, but once I found one participant everything went smooth. A lesson learned is small and medium-sized enterprises are the main target for cyberattacks and finding the right personnel can be an overwhelming process.

Conclusion

Cyberattacks on small and medium-sized enterprises continues to be a growing problem due to the lack of cybersecurity professionals in business (Dolezal, & Tomaskova, 2019). All business with top talented and major resources dedicated to cybersecurity have suffered major cybersecurity conciliations, and organizations that do not have such levels of talented or resources face even greater encounters. Businesses need to find highly skilled workers in the cybersecurity field to help the nation respond more forcefully to the cybersecurity problems it faces. All businesses need to understand their threat situation and the threats they face, report their cybersecurity problems, and employ the most appropriate people to do that work. The purpose of the qualitative case study was to explore what operational strategies CISOs of high-technology companies use to protect their businesses from cyberattacks. Cybersecurity professionals were

appropriate participants for this study because of their experience of cyberattacks on their organizations.

References

Abdo, H., Kaouk, M., Flaus, J.M., & Masse, F. (2018). A safety/security risk analysis approach of industrial control systems: A cyber bowtie-combining new version of attack tree with bowtie analysis. *Computers & Security, 72*, 175-195. doi:10.1016/j.cose.2017.09.004

Abhishta, A., van Rijswijk-Deij, R., & Nieuwenhuis, L. J. (2019). Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers. *ACM SIGCOMM Computer Communication Review*, *48*(5), 70-76. doi:10.1145/3310165.3310175

Aishwarya, K., Pratiksha, S., Hule, P., & Sayli, M. (2018). Survey on Network security. *International Journal of Current Trends in Science and Technology*, *8*(1), 47-53. doi:10.15520/ctst.v8i1.352

Alam, M., Zou, P. X., Stewart, R. A., Bertone, E., Sahin, O., Buntine, C., & Marshall, C. (2019). Government championed strategies to overcome the barriers to public building energy efficiency retrofit projects. *Sustainable Cities and Society*, *44*, 56-69. doi:10.1016/j.scs.2018.09.022

Alcalde-Heras, H., Iturrioz-Landart, C., & Aragon-Amonarriz, C. (2019). SME ambidexterity during economic recessions: the role of managerial external capabilities. *Management Decision*, *57*(1), 21-40. doi:10.1108/MD-03-2016-0170

Aslanidis, P. (2018). Measuring populist discourse with semantic text analysis: an application on grassroots populist mobilization. *Quality & Quantity*, *52*, 1241-1263. doi:10.1007/s11135-017-0517-4

Andraski, M. P., Chandler, C., Powell, B., Humes, D., & Wakefield, S. (2014). Bridging the divide: HIV prevention research and black men who have sex with men. *American Journal of Public Health, 104*, 708-714. Retrieved from www.ajph .aphapublications.org

Argote, L., & Hora, M. (2017). Organizational learning and management of technology. *Production and Operations Management*, *26*, 579-590. doi:10.1111/poms.12667

Argyris, C. (1996). Actionable knowledge: Design causality in the service of consequential theory. *Journal of Applied Behavioral Science, 32,* 390-40. doi:10.1177/0021886396324004

Argyris, C. (1996). Actionable knowledge: Design causality in the service of consequential theory. *Journal of Applied Behavioral Science, 32*, 390-400. doi:10.1177/0021886396324004

Argyris, C. (1976). Leadership, learning, and changing the status quo. *Organizational Dynamics, 4,* 29-43. doi:10.1016/0090-2616(76)90034-6

Argyris, C. (1993). *Knowledge for action: A guides to overcoming barriers to organizational change.* San Francisco, CA: Jossey-Bass Publishers.

Argyris, C. & Schon, D. (1978). *Organizational Learning: A theory of action perspective.* Reading, MA: Addison-Wesley Publishing Co.

Ashford, S. J., Wellman, N., Sully de Luque, M., De Stobbeleir, K. E., & Wollan, M. (2018). Two roads to effectiveness: CEO feedback seeking, vision articulation, and firm performance. *Journal of Organizational Behavior*, *39*(1), 82-95. doi:10.1002/job.2211

Atoum, I., Otoom, A., & Ali, A.A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security, 22,* 251-264. doi:10.1108/IMCS-02-2013-004

Attaran, M., & Woods, J. (2018). Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship*, 1-25. doi:10.1080/08276331.2018.1466850

Baftiu, N. (2017). Cyber security in Kosovo. *European Journal of Economics, 1*, 160-167. Retrieved from www.iipccl.org

Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., & Williams, J. (2017). *Journal of the Operational Research Society, 68*, 780-791. doi:10-1057/jors.2016.37

Barclay, C. (2017). Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica. *Commonwealth Law Bulletin*, *43*(1), 77-107. doi:10.1080/03050718.2017.1310626

Bartlam, B., Waterfield, J., Bishop, A., Holden, M. A., Barlas, P., Ismail, K. M., Kettle, C., Nadine. . . . Foster, N. E. (2018). The role of qualitative research in clinical trial development: the EASE Back study. *Journal of Mixed Methods Research*, *12*, 325-343. doi:10.1177%2F1558689816656740

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153-165. doi:10.1016/j.cose.2016.10.007

Bastardoz, N., & Van Vugt, M. (2019). The nature of followership: Evolutionary analysis and review. The Leadership Quarterly, 30(1), 81-95. doi:10.1016/j.leaqua.2018.09.004

Baumgartner, R.J., & Rauter, R. (2017). Strategic perspectives of corporate sustainability management to develop a sustainable organization. *Journal of Cleaner Production, 140,* 81-92. doi:10.1016/j.jclepro.2016.04.146

Bendovschi, A. (2015). Cyber-attacks-trends, patterns, and security countermeasures. *Procedia Economics and Finance, 28,* 24-31. doi:10.1016/S2212-5671(15)01077-1

Bhardwaj, A., & Goundar, S. (2019). A framework to define the relationship between cyber security and cloud performance. *Computer Fraud & Security*, *2019*(2), 12-19. doi:10.1016/S1361-3723(19)30020-X

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance Issues and Practice*, *40*, 131-158. doi:10.1057/gpp.2014.19

Biswas, B., & Mukhopadhyay, A. (2018). G-RAM Framework for Software Risk Assessment and Mitigation Strategies in Organizations. *Journal of Enterprise Information Management, 31,* 276-299. doi:10.1108/JEIM-05-2017-0069

Boersma, K. S., Dee, L. E., Miller, S. J., Bogan, M. T., Lytle, D. A., & Gitelman, A. I. (2016). Linking multidimensional functional diversity to quantitative methods: A graphical hypothesis-evaluation framework. *Ecology*, *97*, 583-593. doi:10.1890/15-0688

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition. *Computers & Security, 73*, 114-136. doi:10.1016/j.cose.2017.10.013

Burns, J. M. (1978). Leadership. New York, NY: Harper and Row.

Burns, K. A., Reber, T., Theodore, K., Welch, B., Roy, D., & Siedlecki, S. L. (2018). Enhanced early warning system impact on nursing practice: A phenomenological study. *Journal of advanced nursing*, *74*, 1150-1156. doi:10.1111/jan.13517

Burnap, P., French, R., Turner, F., & Jones, K. (2018). Malware classification using self organising feature maps and machine activity data. *Computers & Security, 73,* 399-410. doi:10.1016/j.cose.2017.11.016

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security, 75*, 24-35. doi:10.1016/j.cose.2018.01.015

Cabrera, L. Y., & Reiner, P. B. (2018). A novel sequential mixed-method technique for contrastive analysis of unscripted qualitative data: Contrastive quantitized content analysis. *Sociological Methods & Research*, *47*, 532-548. doi:10.1177/0049124116661575

Caniëls, M. C., Semeijn, J. H., & Renders, I. H. (2018). Mind the mindset! The interaction of proactive personality, transformational leadership and growth mindset for engagement at work. *Career Development International, 23*(1), 48-66. doi:10.1108/CDI-11-2016-0194

Carmeli, A., & Dothan, A. (2017). Generative work relationships as a source of direct and indirect learning from experiences of failure: Implications for innovation agility and product innovation. *Technological Forecasting and Social Change*, *119*, 27-38. doi:10.1016/j.techfore.2017.03.007

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62. doi:10.1111/1468-2346.12504

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

Carugati, A., Fernández, W., Mola, L., & Rossignoli, C. (2018). My choice, your problem? Mandating IT use in large organisational networks. *Information Systems Journal*, *28*(1), 6-47. doi:10.1111/isj.12120

Casini, L. (2018). International regulation of historic buildings and nationalism: the role of UNESCO. *Nations and Nationalism, 24*, 131-147. doi:10.1111/nana.12377

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24-41. doi:10.1016/j.future.2015.09.031

Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*, *9*, 138-151. doi:10.1109/TSC.2015.2491281

Chase, J., Niyato, D., Wang, P., Chaisiri, S., & Ko, R. (2017). A Scalable Approach to

Joint Cyber Insurance and Security-as-a-Service Provisioning in Cloud Computing. *IEEE Transactions on Dependable and Secure Computing, 99.* doi:10.1109/TDSC.2017.2703626

Chen, M., Herrera, F., & Hwang, K. (2018). Cognitive Computing: Human-centered Computing with Intelligence on Clouds. *IEEE Access, 99*, doi:10.1109/ACCESS.2018.2791469

Choi, H., Park., J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81,* 42-51. doi:10016/j.chb.2017.12.001

Choudhary, N. (2018). The role of safety risk management in the UK rail industry when dealing with cyber threats. *International Journal of Safety and Security Engineering, 8*(1), 48-58. doi:10.2495/safe-v8-n1-48-58

Choudhary, R. (2016). Business Continuity Planning: A study of frameworks, standards and guidelines for banks IT services. *International Journal of Emerging Research in Management & Technology, 5*(8). Retrieved from http://www.ermt.net

Chronopoulos, M., Panaousis, E., & Grossklags, J. (2018). An options approach to cybersecurity investment. *IEEE Access*, *6*, 12175-12186. doi:10.1109/ACCESS.2017.2773366

Cho, J. H., & Ben-Asher, N. (2018). Cyber defense in breadth: Modeling and analysis of integrated defense systems. *The Journal of Defense Modeling and Simulation*, *15*, 147-160. doi:10.1177/1548512917699725

Ciocănel, A., Lazăr, F., Munch, S., Harmon, C., Rentea, G. C., Gaba, D., & Mihai, A. (2018). Helping, mediating, and gaining recognition: The everyday identity work

of Romanian health social workers. *Social work in health care*, *57*, 206-219. doi:10.1080/00981389.2018.1426674

Clark, N., & Guiffault, F. (2018). Seeing through the clouds: Processes and challenges for sharing geospatial data for disaster management in Haiti. *International Journal of Disaster Risk Reduction*, *28*, 258-270. doi:10.1016/j.ijdrr.2018.02.019

Comley-White, N., & Potterton, J. (2018). The perceived barriers and facilitators in completing a Master's degree in Physiotherapy. *South African Journal of Physiotherapy*, *74*(1), 1-5. doi:10.4102/sajp.v74i1.445

Cooke, F. L., Wood, G., Wang, M., & Veen, A. (2019). How far has international HRM travelled? A systematic review of literature on multinational corporations (2000–2014). *Human Resource Management Review*, *29*(1), 59-75. doi.org/10.1016/j.hrmr.2018.05.001

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology, 37*(1), 50-65. doi:10.1080/0144929x.2017.1397193

Dahlin, K. B., Chuang, Y. T., & Roulet, T. J. (2018). Opportunity, Motivation, and Ability to Learn from Failures and Errors: Review, Synthesis, and Ways to Move Forward. *Academy of Management Annals*, *12*, 252-277. doi:10.5465/annals.2016.0049

D'Orazio, C. J., Lu, R., Choo, K.K. R., & Vasilakos, A.V. (2017). A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps. *Applied Mathematics and Computation, 293,* 523-544. doi:10.1016/j.amc.2016.02.051

Delery, J. E., & Roumpi, D. (2017). Strategic human resource management, human capital and competitive advantage: is the field going in circles?. *Human Resource Management Journal*, *27*, 1-21. doi:10.1111/1748-8583-12137

Demek, K. C., Raschke, R. L., Janvrin, D. J., & Dilla, W. N. (2018). Do organizations use a formalized risk management process to address social media risk. *International Journal of Accounting Information Systems*, *28*, 31-44. doi:10.1016/j.accinf.2017.12.004

Demertzis, K., IIiadis, L.S., & Anezakis,V. D. (2018). An innovative soft computing system for smart energy grids cybersecurity. *Advances in Building Energy Research, 12*(1), 3-24. doi:10.1080/17512549.2017.1325401

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management, 54*, 452-464. doi:10-1016/j.m.2016.10-002

Ding, D., Han, Q.L., Xiang, Y., Ge, X., & Zhang, X.M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing, 275,* 1674-1683. doi:10.1016/j.neucom.2017.10.009

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior, 68*, 359-367. doi:101016/j.chb.2016.11.044

Dolezal, O., & Tomaskova, H. (2019). Czech Cyber Security System from a view of System Dynamics. *Journal of Cyber Security and Mobility*, *8*, 241-260. doi: 10.13052/jcsm2245-1439.824

Eaton, B., & Millar, R. (2017). Predicting gravel bed river response to environmental change: the strengths and limitations of a regime-based approach. *Earth Surface Processes and Landforms, 42,* 994-1008. doi:10.1002/esp.4058

Eder, G., & Held, M. (2018). Computing positively weighted straight skeletons of simple polygons based on a bisector arrangement. *Information Processing Letters*, *132*, 28-32. doi:10.1016/j.ipl.2017.12.001

El Hussein, M., Jakubec, S. L., & Osuji, J. (2015). Assessing the FACTS: A mnemonic for teaching and learning the rapid assessment of rigor in qualitative research studies. *The Qualitative Report*, *20*, 1182-1184. Retrieved from www.nsuworks.nova.edu

Fachkha, C., & Debbabi, M. (2016). Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Communications Surveys and Tutorials*, *18*(2), 1197-1227. Retrieved from https://spectrum.library.concordia.ca

Felo, A. J., Kim, J. W., & Lim, J. (2018). Can XBRL detailed tagging of footnotes improve financial analysts' information environment. *International Journal of Accounting Information Systems, 28,* 45-48. doi:10.1016/j.accinf.2017.12.003

Fellnhofer, K. (2018). Game-based entrepreneurship education: impact on attitudes, behaviours and intentions. *World Review of Entrepreneurship, Management and Sustainable Development*, *14*, 205-228. doi:10.1504/WREMSD.2018.089066

Fiedler, F. E. (1958). Leader attitudes and group effectiveness. New York: McGraw-Hill.

Fiedler, F. E. (1967). A theory of leadership effectiveness. New York: McGraw-Hill.

Filieri, R., Hofacker, C. F., & Alguezaui, S. (2018). What makes information in online consumer reviews diagnostic over time? The role of review relevancy, factuality, currency, source credibility and ranking score. *Computers in Human Behavior*, *80*, 122-131. doi:10.1016/j.chb.2017.10.039

Finkelstein, L. M., Costanza, D. P., & Goodwin, G. F. (2018). Do your high potentials have potential. The impact of individual differences and designation on leader success. *Personnel Psychology*, *71*(1), 3-22. doi:10.1111/peps.12225

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research*, *18*, 120. doi:10.1186/s12913-018-2915-2

Friday, D., Ryan, S., Sridharan, R., & Collins, D. (2018). Collaborative risk management: a systematic literature review. *International Journal of Physical Distribution & Logistics Management*, *48,* 231-253. doi:10.1108/IJPDLM-01-2017-0035

Frieder, R. E., Wang, G., & Oh, I. S. (2018). Linking job-relevant personality traits, transformational leadership, and job performance via perceived meaningfulness at work: A moderated mediation model. *Journal of Applied Psychology*, *103*, 324. doi:10.1037/apl0000274

Friesen, P., Kearns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont Report. *The American Journal of Bioethics*, *17*(7), 15-21. doi:10.1080/15265161.2017.1329482

Fuller, C. M., Simmering, M. J., Atinc, G., Atinc, Y., & Babin, B. J. (2016). Common methods variance detection in business research. *Journal of Business Research*, *69*, 3192-3198. doi:10.1016/i.jbusres.2015.12.008

García-Sánchez, E., García-Morales, V. J., & Martín-Rojas, R. (2018). Influence of Technological Assets on Organizational Performance through Absorptive Capacity, Organizational Innovation and Internal Labour Flexibility. *Sustainability*, *10*, 770. doi:10.3390/su10030770

Gebauer, H., Saul, C. J., Haldimann, M., & Gustafsson, A. (2017). Organizational capabilities for pay-per-use services in product-oriented companies. *International Journal of Production Economics*, *192*, 157-168. doi:10.1016/j.ijpe.2016.12.007

Gemünden, H. G., Lehner, P., & Kock, A. (2018). The project-oriented organization and its contribution to innovation. *International Journal of Project Management*, *36*, 147-160. doi:10.1016/j.ijproman.2017.07.009

Georgiou, D., & Lambrinoudakis, C. (2017). Security policy rules and required procedures for two crucial cloud computing threats. *International Journal of Electronic Governance*, *9*, 385-403. doi:10.1504/IJEG.2017.088217

Ghazi, C., Nyland, J., Whaley, R., Rogers, T., Wera, J., & Henzman, C. (2018). Social cognitive or learning theory use to improve self-efficacy in musculoskeletal rehabilitation: A systematic review and meta-analysis. *Physiotherapy theory and practice*, 1-10. doi:10.10800/09593985.2017.1422204

Gil, N., & Pinto, J. K. (2018). Polycentric organizing and performance: A contingency model and evidence from megaproject planning in the UK. *Research Policy*, *47*, 717-734. doi:10.1016/respol.2018.02.001

Giusepponi, K., & Tavoletti, E. (2018). Vision and mission statements in Italian universities: results of an empirical investigation on strategic orientation. *Journal of the Knowledge Economy*, *9*, 301-328. doi:10.1007/s13132-015-0343-7

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*, *9*(02), 133. doi:10.4236/jis.2018.92010

Goroff, D., Polonetsky, J., & Tene, O. (2018). Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data. *The ANNALS of the American Academy of Political and Social Science*, *675*(1), 46-66. doi:10.1177/0002716217742605

Grant, R. M. (1996). Prospering in dynamically-competitive environments: Organizational capability as knowledge integration. *Organization science*, *7*(4), 375-387. doi:10.1287/orsc.7.4.375

Green, J., & Thorogood, N. (2018). *Qualitative methods for health research*. Sage.

Greve, H. R., & Teh, D. (2018). Goal selection internally and externally: A behavioral theory of institutionalization. *International Journal of Management Reviews*, *20*(S1). doi:10.1111/ijmr.12138

Greve, H.R., & Seidel, M-D.L. (2014). The thin red line between success and failure: Oath dependence in the diffusion of innovative production technologies. *Strategic Management Journal, 36,* 475-496. doi:10.1002/smj.2232

Grossman, R. L. (2018). A framework for evaluating the analytic maturity of an organization. *International Journal of Information Management*, *38*(1), 45-51. doi:10.1016/i.ijinfomgt.2017.08.005

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy, 20*, 109-122. doi:10.1080/08854726.2014.925660

Grover, V., Chiang, R. H., Liang, T. P., & Zhang, D. (2018). Creating Strategic Business Value from Big Data Analytics: A Research Framework. *Journal of Management Information Systems*, *35*, 388-423. doi:10.1080/07421222.2018.1451951

Gustafsson, R., & Jarvenpaa, S. (2018). Extending community management to industry-university-government organizations. *R&D Management*, *48*(1), 121-135. doi:10.1111/radm.12255

Hadlington, L., & Murphy, K. (2018). Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. *Cyberpsychology, Behavior, and Social Networking, 21*, 168-172. doi:10.1089/cyber.2017.0524

Hamilton, E., Cruz, A. D., & Jack, S. (2017). Re-framing the status of narrative in family research: Towards an understanding of families in business. *Journal of Family Business Strategy, 8*(1), 3-12. doi:10-1016/jfbs.2016.11-001

Han, L., Liu, S., Han, S., Jia, W., & Lei, J. (2018). Owner based malware discrimination. *Future Generation Computer Systems*, *80*, 496-504. doi:10.1016/j.future.2016.05.020

Harrigan, K. R., & DiGuardo, M. C. (2017). Sustainability of patent-based competitive advantage in the US communications services industry. *The Journal of Technology Transfer*, *42*, 1334-1361. doi:10.1007/s10961-016-9515-2

Hasbini, M. A., Eldabi, T., & Aldallal, A. (2018). Investigating the information security management role in smart city organisations. *World Journal of Entrepreneurship, Management and Sustainable Development*, *14*(1), 86-98. doi:10.1108/WJEMSD-07-2017-0042

Hawkins, N. (2018). Resistance, response and recovery. *Computer Fraud & Security*, *2018*(2), 10-13. doi:10.1016/S1361-3723(18)30014-9

Heikkilä, M., Bouwman, H., & Heikkilä, J. (2018). From strategic goals to business model innovation paths: an exploratory study. *Journal of Small Business and Enterprise Development*, *25*(1), 107-128. doi:10.1108/JSBED-03-2017-0097

Henschel, T., & Heinze, I. (2018). Small and Medium-sized Enterprises (SMEs). *Open Innovation And Knowledge Management In Small And Medium Enterprises*, *3*(7), 7-34. doi:10.1142/9789813233591_002

Hersey, P., & Blanchard, K. H. (1969). Life cycle theory of leadership. *Training & Development Journal*, *23*(5), 26-34. Retrieved from http://psycnet.apa.org

Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organisational responses to regulative pressures in information security management: The case of a Chinese

hospital. *Technological Forecasting and Social Change*, *126*, 64-75. doi:10.1016/j.techfore.2017.03.023

Hu, X., Xu, M., Xu, S., & Zhao, P. (2017). Multiple cyber attacks against a target with observation errors and dependent outcomes: Characterization and optimization. *Reliability Engineering & System Safety, 159,* 119-133. doi:10.1016/j.ress.2016.10.025

Hughes, B. B., Bohl, D., Irfan, M., Margolese-Malin, E., & Solórzano, J. R. (2017). ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. *Technological Forecasting and Social Change*, *115*, 117-130. doi:10.1016/j.techfore.2016.09.027

Hulland, J., Baumgartner, H., & Smith, K. M. (2018). Marketing survey research best practices: evidence and recommendations from a review of JAMS articles. *Journal of the Academy of Marketing Science*, *46*, 92-108. doi:10.1007/s11747-017-0532-y

Hutchins, M., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing, 1,* 47-63. doi:10.1016/j.promfg.2015.09.060

Ifinedo, P. (2018). Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions. *Information Resources Management Journal (IRMJ), 31*(1), 53-82. doi:10.4018/IRMJ.2018010103

Irwin, K. C., Landay, K. M., Aaron, J. R., McDowell, W. C., Marino, L. D., & Geho, P. R. (2018). Entrepreneurial orientation (EO) and human resources outsourcing (HRO): A "HERO" combination for SME performance. *Journal of Business Research, 90*, 134-140. doi:10.1016/j.jbusres.2018.05.016

Ismail, W., Alwi, N. H. M., Ismail, R., Bahari, M., & Zakaria, O. (2018). Readiness of Information Security Management Systems (ISMS) Policy on Hospital Staff Using e-Patuh System. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10*(1-11), 47-52. Retrieved from http://www.journal.utem.edu

Jalali, M., & Kaiser, J. (2018). Cyber Resiliency in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research, 20*(5): e10059. doi:10.2196/10059

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

Jaruga, P., Coskun, E., Johnson, W. E., & Kimbrough, K. (2017). Biomarkers of oxidatively induced DNA damage in dreissenid mussels: An ecosystem health assessment tool for the Laurentian Great Lakes. *Environmental Toxicology, 32*(9). doi:10.1002/tox.22427

Javani, B., & Rwelamila, P.D. (2016). Risk management in IT projects-A case of the South African public sector. *International Journal of Managing Projects in Business, 9*(2), 389. doi:10.1108/IJMPB-07-2015-0055

Jayakar, K. (2018). Universal Broadband: Option, Right or Obligation. *Journal of Human*

Values, 24(1), 11-24. doi:10.1177/0971685817733569

Jinno, H., Abe, H., & Iizuka, K. (2017). Consideration of ERP effectiveness: From the perspective of ERP implementation policy and operational effectiveness. *Information*, *8*(1), p. 14. doi:10.3390/info8010014

Johnston, C. M., Wallis, M., Oprescu F. I., & Gray, M. (2017). Methodological considerations related to nurse researchers using their own experience of a phenomenon within phenomenology. *Journal of Advanced Nursing, 73,* 574-584. doi:10.1111/jan.13198

Joo, Y. M., & Tan, T. B. (2018). Smart Cities: A New Age of Digital Insecurity. *Survival, 60*(2), 91-106. doi:10.1080/00396338.2018.1448577

Kaban, E., & Legowo, N. (2018). Audit information system risk management using ISO 27001 framework at private bank. *Journal of Theoretical and Applied Information Technology, 96*(1). Retrieved from http://www.jatit.org

Kakucha, W., & Buya, I. (2018). Information System Security Mechanisms in Financial Management. *Journal of Information and Technology*, *2*(1), 1-16. Retrieved from https://stratfordjournals.org

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security, 25,* 300-329. doi:10.1108/ICS-02-2016-0013

Kark, R., Van Dijk, D., & Vashdi, D. R. (2018). Motivated or Demotivated to Be

Creative: The Role of Self-Regulatory Focus in Transformational and Transactional Leadership Processes. *Applied Psychology*, *67*, 186-224. doi:10.1111/apps.12122

Kern, F. G. (2018). The trials and tribulations of applied triangulation: weighing different data sources. *Journal of Mixed Methods Research*, *12*, 166-181. doi:10,1177/1558689816651032

Kshetri, N. (2018). Introducing the IT Economics Department. *IT Professional*, *20*(1), 83-87. doi:10.1109/MITP.2018.011311501

King Z., Henshel, D., Flora, L., Cains, M.G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring for cybersecurity risk assessment. *Frontiers in Psychology, 9*, 39. doi:10.3389/fpsyg.2018.00039

Kisekka, V., & Giboney, J. S. (2018). The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes. *Journal of Medical Internet Research*, *20*(4). doi:10.2196/jmir.9014

Ko, C., Ma, J., Bartnik, R., Haney, M. H., & Kang, M. (2018). Ethical leadership: An integrative review and future research agenda. *Ethics & Behavior*, *28*, 104-132. doi:10.1080/10508422.2017.1318

Kopaneva, I. M. (2019). Left in the dust: Employee constructions of mission and vision ownership. International Journal of Business Communication, 56(1), 122-145. doi:10.1177/2329488415604457

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*, 691-697. doi:10.1016/j.procs.2017.12.089

Kuo, S. Y., Lin, P. C., & Lu, C. S. (2017). The effects of dynamic capabilities, service capabilities, competitive advantage, and organizational performance in container shipping. *Transportation Research Part A: Policy and Practice*, *95*, 356-371. doi:10.1016/j.tra.2016.11.015

Laureani, A., & Antony, J. (2019). Leadership and Lean Six Sigma: a systematic literature review. Total Quality Management & Business Excellence, 30(1-2), 53-81. doi: 10.1080/14783363.2017.1288565

Latunde, Y. C. (2017). Qualitative Research Methods. In *Research in Parental Involvement*. Palgrave Macmillan US.

Lehto, M. (2018). Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences. *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*, 248. doi:10.4018/978-1-5225-5634-3.ch015

Leiber, M. J., Beaudry-Cyr, M., Peck, J. H., & Mack, K. Y. (2018). Sentencing recommendations by probation officers and judges: An examination of adult offenders across gender. *Women & Criminal Justice*, *28*, 100-124. doi:10.1080/08974454.2017.1297279

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care, 4,* 324-327. doi:10.4103/2249-

4863.161306

Liang, X., Zhao, X., Wang, M., & Li, Z. (2018). Small and Medium-Sized Enterprises Sustainable Supply Chain Financing Decision Based on Triple Bottom Line Theory. Sustainability, 10, 4242. doi:10.3390/su10114242

Li, Y., Chen, H., Liu, Y., & Peng, M. W. (2014). Managerial ties, organizational learning, and opportunity capture: A social capital perspective. *Asia Pacific Journal of Management, 31*, 271-291. doi:10.1007/s10490-012-9330-8

Liu, C. H. S. (2018). Examining social capital, organizational learning and knowledge transfer in cultural and creative industries of practice. *Tourism Management*, *64*, 258-270. doi:10.1016/j.tourman.2017.09.001

Liu, X., Li, Z., Shuai, Z., & Wen, Y. (2017). Cyber attacks against the economic operation of power systems: a fast solution. *IEEE Transactions on Smart Grid*, *8*, 1023-1025. doi:10.1109/TSG.2016.2623983

Liu, X., Shahidehpour, M., Li, Z., Liu, X., Cao, Y., & Li, Z. (2017). Power system risk assessment in cyber attacks considering the role of protection systems. *IEEE Transactions on Smart Grid*, *8*, 572-580. doi:10.1109/TSG.2016.2545683

Locke, C. (2017). Why financial services should accelerate biometrics adoption. *Biometric Technology Today, 2017*(1), 7-9. doi:10-1016/S0969-4765(17)30014-0

Loon, M. (2019). Knowledge management practice system: Theorising from an international meta-standard. *Journal of Business Research*, *94*, 432-441. doi:10.1016/j.jbusres.2017.11.022

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security*, *2017*(4), 18-

20. doi:10.1016/S1361-3723(17)30034-9

Lozano, F. J., Lozano, R., Freire, P., Jiménez-Gonzalez, C., Sakao, T., Ortiz, M. G., Trianni, A., Carpenter, A., & Viveros, T. (2018). New perspectives for green and sustainable chemistry and engineering: Approaches from sustainable resource and energy use, management, and transformation. *Journal of Cleaner Production*, *172*, 227-232. doi:10.1016/j.clepro.2017.10.145

Lucero, J., Wallerstein, N., Duran, B., Alegria, M., Greene-Moton, E., Israel, B., Kastelic, Magarati., M., Oetzel, J., Pearson, C., Schulz, A., Villegas, M., White Hat, E. R. (2018). Development of a mixed methods investigation of process and outcomes of community-based participatory research. *Journal of Mixed Methods Research*, *12*(1), 55-74.

Lucia, W., Sinopoli, B., & Franze, G. (2016). A set-theoretic approach for secure and resilient control of Cyber-Physical Systems subject to false data injection attacks. *Science of Security for Cyber-Physical Systems Workshop*, *12,* 1555-1570. doi:10.1109/SOSCYPS.2016.7580002

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: a systematic review. *Technology and Health Care*, *24*(1), 1-9. doi:10.3233/THC-151102

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*, *19*(1), 19. doi:10.3390/s19010019

Lynch, B. M., McCance, T., McCormack, B., & Brown, D. (2018). The development of the Person-centred Situational Leadership Framework: Revealing the being of person-centredness in nursing homes. *Journal of Clinical Nursing*, *27*, 427-440. doi:10.1111/jocn.13949

Ma, X., Kang, K., Lu, W., Xu, L., & Chen, C. (2018). Research on the access control protocol Priccess design of network privacy protection. *Cluster Computing*, 1-12. doi:10.1007/s10586-017-1681-y

Mahabare Sayli, K. (2018). Survey on network security. *International Journal of Current Trends in Science and Technology, 8*(1), 47-53. doi:10.15520/ctst.v8i1.352.pdf

Mamonov, S., & Triantoro, T. M. (2018). The strategic value of data resources in emergent industries. *International Journal of Information Management, 39*, 146-155. doi:10.1016/j.ijinfomgt.2017.12.004

Mansfield-Devine, S. (2017). Leaks and ransoms–the key threats to healthcare organisations. *Network Security*, *2017*(6), 14-19. doi:10.1016/S1353-4858(17)30062-4

Martin, K. (2018). Trust and the Online Market Maker: A comment on Etzioni's cyber trust. *Journal of Business Ethics,* 1-4. doi:10.1007/s10551-018-3780-y

Matt, M., Gaunand, A., Joly, P. B., & Colinet, L. (2017). Opening the black box of impact–Ideal-type impact pathways in a public agricultural research organization. *Research Policy*, *46*, 207-218. doi:10.1016/j.respoi.2016.09.016

Matthies, B., & Coners, A. (2018). Double-loop learning in project environments: An implementation approach. *Expert Systems with Applications*, *96*, 330-346. doi:10.1016/j.eswa.2017.12.012

McClory, S., Read, M., & Labib, A. (2017). Conceptualising the lessons-learned process rin project management: Towards a triple-loop learning framework. *International Journal of Project Management*, *35*, 1322-1335. doi:10.1016/ijproman.2017.05.006

McNamara, P., Pazzaglia, F., & Sonpar, K. (2018). Large-scale events as catalysts for creating mutual dependence between social ventures and resource providers. *Journal of Management*, *44*, 470-500. doi:10.1177/0149206314563983

Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management, 40,* 54-66. doi:10.1016/j.ijinfomgt.2018.01.001

Moore, T. P., McArthur, M., & Noble-Carr, D. (2018). More a marathon than a hurdle: towards children's informed consent in a study on safety. *Qualitative Research*, *18*(1), 88-107. doi:10.1177/1468794117700708

Müller, R., Sankaran, S., Drouin, N., Vaagaasar, A. L., Bekker, M. C., & Jain, K. (2018). A theory framework for balancing vertical and horizontal leadership in projects. *International Journal of Project Management*, *36*(1), 83-94. doi:10.1016/j.ijproman.2017.07.003

Mohr, J. J., & Metcalf, E. C. (2018). The business perspective in ecological restoration: issues and challenges. *Restoration Ecology*, *26*, 381-390. doi:10.1111/rec.12562

Moore, C., Mayer, D. M., Chiang, F. F., Crossley, C., Karlesky, M. J., & Birtch, T. A. (2019). Leaders matter morally: The role of ethical leadership in shaping employee moral cognition and misconduct. *Journal of Applied Psychology*, *104*(1), 123. doi:10.1037/apl0000341

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9-18. doi:10.1080/13814788.2017.1375091

Nambisan, S. (2018). Architecture vs. ecosystem perspectives: Reflections on digital innovation. *Information and Organization, 28,* 104-106. doi:10.1016/j.infoandorg.2018.04.003

Nieuwboer, M. S., van der Sande, R., van der Marck, M. A., Olde Rikkert, M. G., & Perry, M. (2019). Clinical leadership and integrated primary care: A systematic literature review. *European Journal of General Practice*, *25*(1), 7-18. doi:10.1080/13814788.2018.1515907

Nishigaki, M. (2018). Humanics information security. Concurrency and Computation: *Practice and Experience, 30*(2). doi:10.1002/cpe.4274

Nissinboim, N., & Naveh, E. (2018). Process standardization and error reduction: A revisit from a choice approach. *Safety Science*, *103*, 43-50. doi:10.1016/j.ssci.2017.11.015

Nordin, P., Kork, A. A., & Koskela, I. (2017). Value-based healthcare measurement as a context for organizational learning: Adding a strategic edge to assess health outcome. *Leadership in Health Services*, *30*, 159-170. doi:10.1108/LHS-10-2016-0053

Northouse, P. G. (2016). *Leadership: Theory and practice*. Sage publications.

Northouse, P. G. (2018). *Leadership: Theory and practice*. Sage publications.

O Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. Methods in Ecology and Evolution, 9(1), 20-32. doi:10.1111/2041-210X.12860

Olano, J. (2018). The Struggle to Define Privacy Rights and Liabilities in a Digital World and the Unfortunate Role of Constitutional Standing. *University of Miami Law Review*, *72*, 1025. Retrieve from: https://repository.law.miami.edu

Osborn, E., & Simpson, A. (2017). On small-scale IT users' systems architectures and cybersecurity: A UK case study. *Computers & Security, 70,* 27-50. doi:10.1016/j.cose.2017.05.001

Page, J., Kaur, M., & Waters, E. (2017). Directors' liability survey: Cyber attacks and data loss—a growing concern. *Journal of Data Protection & Privacy*, *1*, 173-182. doi:10.1016/j.cose.2017.05.001

Palmas, W. (2018). Who protects participants in non-inferiority trials when the outcome is death. *Research Ethics*, *14*(1), 10-15. doi:10.1177/1747016118764304

Para-González, L., Jimenez-Jimenez, D., & Martínez-Lorente, A. R. (2018). Exploring

the mediating effects between transformational leadership and organizational performance. *Employee Relations*, *40*, 412-432. doi:10.1108/ER-10-2016-0190

Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2018). Identifying core concepts of cybersecurity: Results of two Delphi processes. *IEEE Transactions on Education*, *61*(1), 11-20. doi:10.1109/TE.2017.2715174

Park, K., Woo, S., Moon, D., & Choi, H. (2018). Secure Cyber Deception Architecture and Decoy Injection to Mitigate the Insider Threat. *Symmetry*, *10*(1), 14. doi:10.3390/sym10010014

Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, *38*, 226-241. doi:10.1111/risa.12844

Paul, S. (2017). Reinforcing your SME against cyberthreats. *Computer Fraud & Security*, *2017*(10), 13-15. doi:10.1016/S1361-3723(17)30091-X

Pawlak, P., & Barmpaliou, P. N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, 1-22. doi:10.1080/23738871.2017.1294610

Pearce, P., Ensafi, R., Li, F., Feamster, N., & Paxson, V. (2018). Toward Continual Measurement of Global Network-Level Censorship. *IEEE Security & Privacy*, (1), 24-33. doi:10.1109/MSP.2018.1331018

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From Naive Trust to Risk Awareness. *Trends in Biotechnology*, *36*(1), 4-7. doi:10.1016/j.tibtech.2017.10.012

Penuel, W. R., Farrell, C. C., Allen, A. R., Toyama, Y., & Coburn, C. E. (2018). What research district leaders find useful. *Educational Policy*, *32*, 540-568. doi:10.1177/0895904816673580

Peters, L. H., Hartke, D. D., & Pohlmann, J. T. (1985). Fiedler's contingency theory of leadership: An application of the meta-analysis procedures of Schmidt and Hunter. *Psychological Bulletin, 97,* 274-285. doi:10.1037/0033-2909.97.2.274

Petrila, J. (2018). Turning the law into a tool rather than a barrier to the use of administrative data for evidence-based policy. *The ANNALS of the American Academy of Political and Social Science, 675*(1), 67-82. doi:10.1177/0002716217741088

Philips, D. M., Mazzuchi, T. A., & Sarkani, S. (2018). An architecture, system engineering, and acquisition approach for space system software resiliency. *Information and Software Technology, 94*, 150-164. doi:10.1016/j.infsof.2017.10.006

Pisano, G. P. (2017). Toward a prescriptive theory of dynamic capabilities: connecting strategic choice, learning, and competition. *Industrial and Corporate Change*, *26*, 747-762. doi:10.1093/icc/dtx026

Pokorny, J. J., Norman, A., Zanesco, A. P., Bauer-Wu, S., Sahdra, B. K., & Saron, C. D. (2018). Network analysis for the visualization and analysis of qualitative data. *Psychological methods*, *23*(1), 169. doi:10.1037/met0000129

Ponemon Institute (2017). 2017 Cost of Data Breach Study. Global Overview, Retrieve from http://www.ibm.com

Puttick, S. (2017). Performativity, guilty knowledge, and ethnographic intervention. *Ethnography and Education, 12*(1), 49-63. doi:10.1080/17457823.2015.1110039

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44-55. doi:10.1016/j.cosrev.2018.05.003

Qi, C., & Chau, P. Y. K. (2018). Will enterprise social networking systems promote knowledge management and organizational learning? An empirical study. *Journal of Organizational Computing and Electronic Commerce, 28*(1), 31-57 doi:10.1080/10919392.2018.1407081

Rahman, R. (2017). How the legal fraternity should respond to modern cybercrimes. Mediterranean *Journal of Social Sciences, 8*(1), 41. doi:10.5901/mjss.2017.v8n1p41

Reid, M., Walsh, C., Raubenheimer, J., Bradshaw, T., Pienaar, M., Hassan, C., Nyoni, M., re& Le Roux, M. (2018). Development of a health dialogue model for patients with diabetes: A complex intervention in a low-/middle income country. *International Journal of Africa Nursing Sciences*, *8*, 122-131. doi:10.1016/j.ijans.2018.05.002

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two Strategies for Qualitative Content Analysis: An Intramethod Approach to Triangulation. *Qualitative health research*, *28*(5), 824-831. doi:10.1177/1049732317753586

Rezaei, A., Allameh, S. M., & Ansari, R. (2018). Impact of knowledge creation and organisational learning on organisational innovation: an empirical investigation. *International Journal of Business Innovation and Research*, *16*(1), 117-133. doi:10.1504/IJBIR.2018.091087

Riazi, A. M. (2018). Mixed methods approaches to studying second language writing. *The TESOL Encyclopedia of English Language Teaching*, 1-6. doi:10.1002/9781118784235.eelt0562

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

Rodgers, S., Wang, Z., Maras, M. A., Burgoyne, S., Balakrishnan, B., Stemmle, J., & Schultz, J. C. (2018). Decoding Science: Development and Evaluation of a Science Communication Training Program Using a Triangulated Framework. *Science Communication*, *40*(1), 3-32. doi:10.1177/1075547017747285

Ross, M. W., Iguchi, M. Y., & Panicker, S. (2018). Ethical aspects of data sharing and research participant protections. *American Psychologist*, *73*(2), 138. doi:10.1037/amp0000240

Rostamzadeh, R., Ghorabaee, M. K., Govindan, K., Esmaeili, A., & Nobar, H. B. K. (2018). Evaluation of sustainable supply chain risk management using an

integrated fuzzy TOPSIS-CRITIC approach. *Journal of Cleaner Production, 175*, 651-669. doi:10.1016/j.jclepro.2017.12.071

Rubin, B, & Xu, A. (2016). Cybersecurity enforcement actions: is the SEC bringing strict liability cases. *Journal of Investment Compliance, 17*, 112-116. doi:10.1108/JOIC-02-2016-0004

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

Sandor, D., Fulton, S., Engel-Cox, J., Peck, C., & Peterson, S. (2018). System Dynamics of Polysilicon for Solar Photovoltaics: A Framework for Investigating the Energy Security of Renewable Energy Supply Chains. Sustainability, 10(1), 160. doi:10.3390/su10010160

Sanjari, M., Bahramnezhad, F., Fomani, F. K., Shoghi, M., & Cheraghi, M. A. (2014). Ethical challenges of researchers in qualitative studies: the necessity to develop a specific guideline. *Journal of Medical Ethics and History of Medicine*, *7*, 14. doi:10.1177/1745691617706516

Sarkar, B. K., & Sana, S. S. (2018). A conceptual distributed framework for improved and secured healthcare system. *International Journal of Healthcare Management*, 1-13. doi:10.1080/20479700.2017.1422338

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., Petrozzino, C., & Zuk, M. (2018). The Evolving State of Medical Device Cybersecurity.

Biomedical Instrumentation & Technology, 52(2), 103-111. doi:10.2345/0899-8205-52-2-103

Shaw, S. D., & Bagozzi, R. P. (2018). The neuropsychology of consumer behavior and marketing. Consumer Psychology Review, 1(1), 22-40. doi:10.1002/arcp.1006

Sheperis, C. J., Young, J. S., & Daniels, M. H. (2016). Counseling research: Quantitative, qualitative, and mixed methods. Pearson.

Sieber, U., & Neubert, C. W. (2017). Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty. *Max Planck Yearbook of United Nations Law Online, 20*, 239-321. doi:10.1163/13894633_02001010

Sim, J. J. (2017). Moving towards a mixed-method approach to educational assessments. *Academic Medicine, 92,* p. 726. doi:10.1097/ACM.0000000000001680

Simonin, B. L. (2017). N-loop learning: part II–an empirical investigation. *The Learning Organization*, *24*(4). doi:10.1108/TLO-12-2016-0100

Shakya, S., & Gupta, A. (2018). Concerns on Information System and Security Audit. *Journal of Advanced College of Engineering and Management*, *3*, 127-135. doi:10.3126/jacem.v3i0.18966

Shekhar, P., Prince, M., Finelli, C., Demonbrun, M., & Waters, C. (2018). Integrating quantitative and qualitative research methods to examine student resistance to active learning. *European Journal of Engineering Education*, 1-13. doi:1080/03043797.2018.1438988

Škrjanc, I., Ozawa, S., Ban, T., & Dovžan, D. (2018). Large-scale cyber attacks monitoring using Evolving Cauchy Possibilistic Clustering. *Applied Soft Computing*, *62*, 592-601. doi:10.1016/j.asoc.2017.11.008

Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: Problems and opportunities within sport and exercise psychology. *International Review of Sport and Exercise Psychology*, *11*, 101-121. doi:10.1080/1750984X.2017.1317357

Smith, D. H., Kuntz, J., DeBar, L., Mesa, J., Yang, X., Boardman, D., & Schneider, J. (2018). A qualitative study to develop materials educating patients about opioid use before and after total hip or total knee arthroplasty. *Journal of Opioid Management*, *14*(3), 183-190. Retrieved from http://www.wmpllc.

Smith, E., Corzine, S., Racey, D., Dunne, P., Hassett, C., & Weiss, J. (2016). Going beyond Cybersecurity Compliance: What power and utility companies really need to consider. *IEEE Power and Energy Magazine*, *14*(5), 48-56. doi:10.1109/MPE.2016.2573898

Smith, K. H., Méndez Mediavilla, F. A., & White, G. L. (2018). The Impact of Online Training on Facebook Privacy. *Journal of Computer Information Systems*, *58*, 244-252. doi:10.1080/08874417.2016.1233001

Spicker, P. (2018). The Real Dependent Variable Problem: The Limitations of Quantitative Analysis in Comparative Policy Studies. *Social Policy & Administration*, *52*, 216-228. doi:10.1111/spol.12308

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975. doi:10.1016/j.future.2016.11.031

Sun, C.C., Hahn, A., & Liu, C.C. (2018). Cyber security of power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems, 99,* 45-56. doi:10.1016/j.ijepes.2017.12.020

Symantec Corporation. (2017). *Internet security threat report (ISTR) 2017* (Volume 22). Mountain View, CA: Author. Retrieved from https://www.symantec.com

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

Thomas, J. E., & Galligher, G. C. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. *Computer and Information Science*, *11*(1), 14. doi:10.5539/cis.v11n1p14

Timms, K. (2017). BYOD must be met with a wider appreciation of the cyber-security threat. *Computer Fraud & Security*, *2017*(7), 5-8. doi:10.1016/S1361-3723(17)30058-1

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The Privacy Implications of Cyber Security Systems: A Technological Survey. *ACM Computing Surveys (CSUR)*, *51*(2), 36. doi:10.1145/3172869

Trotter, M. J., Salmon, P. M., Goode, N., & Lenné, M. G. (2018). Distributed Improvisation: A systems perspective of improvisation 'epics' by led outdoor activity leaders. *Ergonomics*, *61*, 295-312. doi:10.1080/00140139.2017.1355071

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283-297. doi:10.1016/j.chb.2017.10.007

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in Cybersecurity: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. *Frontiers in Psychology*, *9*, 691. doi:10.3389/fpsyg.2018.00691

Von Solms, B., & von Solms, R. (2018). Cybersecurity and information security–what goes where. *Information & Computer Security*, *26*, 2-9. doi:10.1108/ICS-04-2017-0025

Voskoboinicov, S., & Melnyk, S. (2018). Cyber security in the modern sociation and improvement of preparation of future factors in the field of competent approach. *Social Work and Education, 5*(1). doi:10.25128/2520-6230.18.1.10

Wadhwa, A., & Arora, N. (2017). A Review on Cyber Crime: Major Threats and Solutions. *International Journal of Advanced Research in Computer Science*, *8*(5). doi:10.26483/ijarcs.v8i5.4067

Wang, Y., Kung, L., & Byrd, T. A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change*, *126*, 3-13. doi:10.1016/j.techfore.2015.12.019

Wang, X., Wang, R., Wang, L., Chen, X., & Geng, X. (2018). An efficient single-loop strategy for reliability-based multidisciplinary design optimization under non-probabilistic set theory. *Aerospace Science and Technology*, *73*, 148-163. doi:10.1016/j.ast/2017.11.046

Wang, M., Wu, B., Kirschner, P. A., & Spector, J. M. (2018). Using Cognitive Mapping to Foster Deeper Learning with Complex Problems in a Computer-Based Environment. *Computers in Human Behavior*. doi:10.1016/j.chb.2018.01.024

West, J. (2018). A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies. *Journal of Agricultural & Food Information*, 1-24. doi:10.1080/10496505.2017.1417859

Whitten, D. (2016). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems*, *48*(3), 15-19. doi:10.1080/08874417.2008.11646017

Wiengarten, F., & Longoni, A. (2018). How does uncertainty affect workplace accidents? Exploring the role of information sharing in manufacturing networks. *International Journal of Operations & Production Management*, *38*, 295-310. doi:10.1108/ijopm-07-2015-0431

Wright, M., Tartari, V., Huang, K. G., Di Lorenzo, F., & Bercovitz, J. (2018). Knowledge

worker mobility in context: Pushing the boundaries of theory and methods. *Journal of Management Studies*, *55*, 1-26. doi:10.1111/joms.12316

Wu, T. T. (2018). Improving the effectiveness of English vocabulary review by integrating ARCS with mobile game-based learning. *Journal of Computer Assisted Learning*, *123*(3), 1-9. doi:10.111/jcal.12244

Xie, J., Hong, T., Laing, T., & Kang, C. (2017). On normality assumption in residual simulation for probabilistic load forecasting. *IEEE Transactions on Smart Grid, 8*, 1046-1053. doi:10.1109/TSG.2015.2447007

Yamin, M., & Sen, A. A. A. (2018). Improving Privacy and Security of User Data in Location Based Services. *International Journal of Ambient Computing and Intelligence (IJACI)*, *9*(1), 19-42. doi:10.4018/IJACI.2018010102

Yang, Y., Pankow, J., Swan, H., Willett, J., Mitchell, S. G., Rudes, D. S., & Knight, K. (2018). Preparing for analysis: a practical guide for a critical step for procedural rigor in large-scale multisite qualitative research studies. *Quality & Quantity*, *52*, 815-828. doi:10.1007/s11135-017.0490-y

Yeh, C. L. (2018). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*, *42*, 282-292. doi:10.1016/j.telpol.2017.12.001

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

Yin, H., Guo, D., Wang, K., Jiang, Z., Lyu, Y., & Xing, J. (2018). Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm. *IEEE Network*, *32*, 112-117. doi:10.1109/MNET.2018.1700172

Zetter, K. (2014). Sony Got Hacked Hard: What we know and don't know so far. Retrieved from http://www.wired.com

Zhang, W., Wang, Z., Liu, Y., Ding, D., & Alsaadi, F. E. (2018). Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks. *International Journal of Robust and Nonlinear Control*, *28*(1), 53-67. doi:10-1002/rnc.3855

Zhai, Y. M., Sun, W. Q., Tsai, S. B., Wang, Z., Zhao, Y., & Chen, Q. (2018). An Empirical Study on Entrepreneurial Orientation, Absorptive Capacity, and SMEs' Innovation Performance: A Sustainable Perspective. *Sustainability*, *10*, 314. doi:10.3390/su10020314

Zhao, X., Miers, I., Green, M., & Mitrani-Reiser, J. (2018). Modeling the cybersecurity of hospitals in natural and man-made hazards. *Sustainable and Resilient Infrastructure*, 1-14. doi:10.1080/23789689.2018.1448666

Zhu, S., Song, J., Hazen, B. T., Lee, K., & Cegielski, C. (2018). How supply chain analytics enables operational supply chain transparency: An organizational information processing theory perspective. *International Journal of Physical Distribution & Logistics Management, 47*(1), 47-68. doi:10.1108/IJPDLM-11-2017-0

Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for*

Security Research, 1-29. doi:10.1007/s441125-019-00039-8

Appendix A: Interview Protocol

I started the interview protocol by sending the letter of invitation, after I made contact with the participant, I will send the participant copy of the consent form. When I received the copy of the consent form back, I called the participant. Introduce the interview, research topic over lunch and explain the purpose and scope of the study. Assure the participants that I will keep all the collected information confidential and inform the participant of the right to stop the interview.

The questions for the interview are as follows:

Demographic Questions:

1. What is your age?
2. Where were you born?
3. What is your highest level of education?
4. How long in the current organization?
5. How many years of experience as a business leader?

Strategic Research Questions

1. What strategies are you using to secure your business from cyberattacks?
2. What are the key challenges to implementing your operational strategies for preventing cyberattacks?
3. How do you address the key challenges to implementing your successful strategies to mitigate cyberattacks?
4. How long has your business been in existence?
5. What type of training do you have in place for your employees about cyber-

attacks?

6. What type of cyberattacks strategies would you like to implement but have not implemented?
7. What additional information on cybersecurity strategies would you like to provide?

Wrap up the interview by thanking the participant and schedule follow-up for member checking interview.

Follow-up and Member Checking Interview

Introduce follow-up interview and set the stage over coffee.

Share a copy of the succinct synthesis for each question and interpretation.

Ask a probing question related to any information that I found during the interview and related to the research topic.

Walkthrough, each question, read the interpretation and ask: Did I miss anything? Or, what would you like to add?

Wrap up the follow-up interview by thanking the participant.

Appendix B: Interview Questions

The central research question for this proposed study is: what operational strategies do CISOs of high-technology companies use to protect their businesses from cyberattacks?

The questions for the interview are as follows:

Demographic Questions:

1. What is your age?
2. What is your highest level of education?
3. How long in the current organization?
4. How many years of experience as a business leader?

Strategic Research Questions

5. What strategies are you using to secure your business from cyberattacks?
6. What are the key challenges to implementing your operational strategies for preventing cyberattacks?
7. How do you address the key challenges to implementing your successful strategies to mitigate cyberattacks?
8. How long has your business been in existence?
9. What type of training do you have in place for your employees about cyber-attacks?

The questions for the interview are as follows:

Demographic Questions:

6. What is your age?

7. Where were you born?
8. What is your highest level of education?
9. How long in the current organization?
10. How many years of experience as a business leader?

Strategic Research Questions

8. What strategies are you using to secure your business from cyberattacks?
9. What are the key challenges to implementing your operational strategies for preventing cyberattacks?
10. How do you address the key challenges to implementing your successful strategies to mitigate cyberattacks?
11. How long has your business been in existence?
12. What type of training do you have in place for your employees about cyber-attacks?
13. What type of cyberattacks strategies would you like to implement but have not implemented?
14. What additional information on cybersecurity strategies would you like to provide?

Wrap up the interview by thanking the participant and schedule follow-up for member checking interview.