2019

Cybersecurity Strategies to Protect Information Systems in Small Financial Institutions

Johnny Fadel Rawass
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Johnny Rawass

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. Ronald Jones, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Rollis Erickson, Committee Member, Doctor of Business Administration Faculty

Dr. Judith Blando, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Cybersecurity Strategies to Protect Information Systems in Small Financial Institutions

by

Johnny Rawass

MMI, University of Phoenix, 2007

BBA, Lebanese University, 1992

BBA, Lebanese University, 1990

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2019

Abstract

Leaders of financial institutions face challenges in protecting data because of the increased use of computer networks in the commerce and governance aspects of their businesses. The purpose of this single case study was to explore the strategies that leaders of a small financial institution used to protect information systems from cyber threats. The actor-network theory was the conceptual framework for this study. Data were collected through face-to-face, semistructured interviews with 5 leaders of a small financial institution in Qatar and a review of company documents relevant to information security, cybersecurity, and risk management. Using thematic analysis and Yin's 5-step data analysis process, the 4 emergent key theme strategies were information security management, cybersecurity policy, risk management, and organizational strategy. The findings of this study indicate that leaders of financial institutions protect their information systems from cyber threats by effectively managing information security practices; developing robust cybersecurity policies; identifying, assessing, and mitigating cybersecurity risks; and implementing a holistic organizational strategy. The protection of information systems through reductions in cyber threats can improve organizational business practices. Leaders of financial institutions might use the findings of this study to affect positive social change by decreasing data breaches, safeguarding consumers' confidential information, and reducing the risks and costs of consumer identity theft.

Cybersecurity Strategies to Protect Information Systems in Small Financial Institutions

by

Johnny Rawass

MMI, University of Phoenix, 2007

BBA, Lebanese University, 1992

BBA, Lebanese University, 1990

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2019

Dedication

I dedicate this study to a real role model, HH the Father Emir Sheikh Hamad Bin Khalifa Al-Thani, for his extreme loyalty and commitment to the Qatari community and for his wise and determined leadership in developing Qatar into a center of attraction for the entire world. HH, the former Emir of Qatar, demands the highest standards for the country's stability, sustainable growth, and a secure economy. This dedication is a token of respect and appreciation for the useful international role played by Qatar under the guidance of HH Sheikh Hamad and for the Qatari people who provided excellent opportunities to many expatriates, such as me, to contribute in the cumbersome process of development of Qatar. I extend my gratitude and respect to HH the Emir Sheikh Tamim Bin Hamad Al-Thani, who is still leading Qatar under the same strategy set by the Father Emir and excelling in protecting the benefits of the state of Qatar and its stability and growing economy, protecting the human rights, and Qatar International positioning by his 2030 wise and promising vision.

I dedicate this study to my family who motivated me to undertake multiple academic investigations and to share my research with technicians, business leaders, and members of the government to highlight the benefits of enhancing the security of information and cybersecurity protection. My primary concern was to offer a realistic and efficient business study that would provide a benefit to Qatar's community and its operating companies, especially its financial institutions, as part of our gratitude to this generous and welcoming country.

Acknowledgments

I express gratitude to my wife May and children Joey, Jenny, and Charbel Rawass for their support during my absences when traveling to residencies and the long hours of studying and gathering the necessary information for the success of this study. I wish to show my appreciation for my committee chairperson, who always assisted me with every phase and contributed to the development of a valuable and credible study.

I express my gratitude and appreciation to my professors, especially my chair Dr. Ronald Jones; my committee members, Dr. Greg Washington, Dr. Denise Land, Dr. Rollis Erickson, and Dr. Judith Blando; the entire Walden University support team; and Dr. Susan Davis, the doctoral program director of Walden University for their patience and guidance through the completed courses. I appreciate the high quality of teaching and academic professionalism shown by the instructors at Walden University in maintaining high educational standards. Finally, I express thanks to the mighty God for his blessings and for supplying me with the proper guidance and strength to follow this journey in my life and to achieve success.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Cybersecurity has challenged business leaders and policymakers of international relations in the digital information age (Carr, 2016). Reid and Van Niekerk (2014) stated the term *cybersecurity* was interchangeable with the term *information security*. Reid and Van Niekerk defined cybersecurity as the collection of instruments, strategies, security paradigms, security precautions, risk management tactics, activities, preparation, best practices, guarantees, and technologies used to defend the cyber atmosphere, institutes, and user data. Paulsen (2016), however, stated that no widely accepted definition for cybersecurity exists. Business leaders noted that cyber threats are more frequent and damaging to the profitability of businesses (Manworren, Letwat, & Daily, 2016). Business leaders have noted that cybersecurity is a social, technical, and economic issue (Prince, 2018). Udroiu (2018) pointed out that infrastructure, hardware, software, policies, and information are levels of an organization in which business leaders implement cybersecurity programs. The purpose of this study was to explore strategies that some leaders of a small financial institution use to protect information systems from cyber threats.

Background of the Problem

Technology and communications usage have evolved in financial institutions. At the beginning of the digital economy era, traditional companies transitioned to Internet businesses to have a presence on the World Wide Web (Bernik, 2014). The possibilities of the Internet allowed public and private business to establish operations through online electronic data systems (Bernik, 2014). Business leaders face challenges in protecting

data because of the increased use of computer networks in the commerce and governance of organizations (Choucri, Madnick, & Ferwerda, 2013). Atoum and Otoom (2016) noted that implementing information systems remained a challenge for business leaders in every country. Researchers have pointed out the global interest and importance of cybersecurity (Von Solms & Van Niekerk, 2013). In a 2016 report, Symantec business leaders stated 43% of spear phishing attacks targeted businesses with 1–250 employees, up from 34% in 2014 (Paulsen, 2016). Cybercriminals used small businesses to access the more massive corporations' data (Paulsen, 2016). Neghina and Scarlat (2013) explained that some cybercriminals are disgruntled employees who physically damage their employers' computer hardware. Flowers, Zeadally, and Murray (2013) stated that cybercriminals attack private and public networks using a variety of computer hardware and software tools. The security of a business's information systems infrastructure is fundamental in the foreign growth of the business because managers depend on sophisticated knowledge and resourceful communication for decision-making in a globalized business setting (Lee, Oh, & Lee, 2017).

Cybercrime is high in the Middle East (Kshetri, 2016). Cybercrimes committed in the Gulf Arab states cost organizations $1 billion annually (Kshetri, 2016). Cybercriminals' motivations for hacking are financial, social, and political (Kshetri, 2016). Information technology plays a vital role in organizational workflow, and management must understand the risk of data breaches (Kshetri, 2016).

Problem Statement

Cybersecurity has been a challenge for Qatar's economic development (Ali, 2019). Thirty-nine percent of Qatari businesses do not have cybersecurity policies in place to combat cyber threats (Benmamoun, Sobh, Singh, & Moura, 2016). The general business problem was that leaders of small financial institutions who do not adopt adequate cybersecurity strategies experience reduced economic growth. The specific business problem was that some leaders of small financial institutions lack strategies to protect information systems from cyber threats.

Purpose Statement

The purpose of this qualitative single case study was to explore the strategies that leaders of a small financial institution use to protect information systems from cyber threats. The target population consisted of business leaders from a small financial institution in Doha, Qatar, who have successfully implemented strategies to protect information systems from cyber threats. The implications for social change include the potential for business leaders to reduce data breaches, safeguard the confidential information of consumers, and reduce the risk and costs of consumer identity theft.

Nature of the Study

The design of this study involved a qualitative single case study research. I used semistructured interviews and company documentation to obtain data regarding the strategies that leaders of a small financial institution use to protect information systems from cyber threats. Scholars use the qualitative research method to understand the deeper meaning of a phenomenon through open discourse with participants (Lewis, 2015). The

qualitative method was appropriate for this study because the purpose of the research was to provide a deeper understanding of the strategies that leaders use to protect information systems from cyber threats. Investigators conducting a quantitative method study seek to collect numeric data for hypothesis testing through statistical analysis (Denzin, 2012; Scrutton & Beames, 2015). I rejected the quantitative method for this study because collecting and analyzing numeric data was not an appropriate means to explore the strategies some leaders of a small financial institution use to protect information systems from cyber threats. The mixed-method approach is suitable if a researcher's purpose is to use both qualitative and quantitative methods to address the problem and answer the research question (Siddiqui & Fitzgerald, 2014). The mixed-method approach was not suitable because this study will not consist of a combination of the qualitative and quantitative methods to conduct the research.

Scholars using the case study approach need various sources of data collection, such as public or private records, interviews, and observations (Morse, 2015). Scholars use a case study design to capture in-depth details regarding a phenomenon occurring in a real world, contextual setting (Yin, 2018). In this study, I used a case study design to conduct an in-depth study of a phenomenon in a real world, bounded setting. Ethnographic investigators engage themselves in the traditions and culture of the sample population as active participants (Samnani & Singh, 2013). An ethnographic design was not suitable for this study because my immersion in the financial institution's culture was not an appropriate means to collect data aligned with the research question. The focus of this study was on cybersecurity strategies used in small financial institutions, not the

culture. Scholars focus on the lived experiences of participants in phenomenological research designs (Reiter, Stewart, & Bruce, 2011). The purpose of this study was to explore the cybersecurity strategies leaders used, not their lived experiences; therefore, I rejected the phenomenological design.

Research Question

The research question for this study is the following: What strategies do leaders of a small financial institution use to protect information systems from cyber threats?

Interview Questions

The interview questions I asked of the study participants to obtain data for this study were the following:

1. What strategies do you use to protect information systems from cyber threats?

2. How do you integrate your strategies to protect information systems from cyber threats into your organizational policies?

3. What is your perspective regarding the extent of cybersecurity strategies needed to protect your information systems from cyber threats?

4. How are your strategies to protect information systems from cyber threats communicated to your employees?

5. How do you tailor your strategies to protect information systems from internal cyber threats?

6. How do you tailor your strategies to protect information systems from external cyber threats?

7. What added information can you offer about the strategies you use to protect information systems from cyber threats?

Conceptual Framework

I chose actor-network theory (Law, 1992) as the conceptual framework for this research study. The purpose of actor-network theory is to give a complete model of the innovation procedure (Young, Borland, & Coghill, 2012). Social scientists use actor-network theory to aid in the understanding of how systems construct fundamental and useful adjustments (Young et al., 2012). Researchers and practitioners use actor-network theory to aid with surmounting standstills and systems rigor (Young et al., 2012). The theoretical paradigms of actor-network theory are heterogeneous networks of humans and nonhuman actors (Jihoon, Kyoung-Yun, & Ohbyung, 2015). Scholars use actor-network theory to explore how systems or organizations derived as one to form assemblies or networks of relations and connections (Parker, 2017). Rocci (2014) stated that researchers use actor-network theory to track the multipart interplay of humans and digital technology to give a focus on the relationship between nonhumans and humans that encapsulated the arbitrated nature of modern life in an evolved technological culture. Researchers and business leaders use actor-network theory to help explain how sociotechnical humanchine networks, formed of humans and technologies as actors, overlap through conversion and create an agency (Rocci, 2014). The humanchine network is the dichotomy of relations between agency, structure, human, and technology (Brooks, Atkinson, & Wainwright, 2008). Balzacq and Cavelty (2016) stated that cyber incidents and international politics relate to actor-network theory. Balzacq and Cavelty

defined actor-network theory as a diverse conglomerate of ideas with beginnings in science and technology research. Initially established to comprehend developments of innovation and knowledge formation in science and technology, actor-network theory was used by social scientists on current work in science, technology, and science to study large technological systems (Cavalheiro & Joia, 2016). Researchers and practitioners use actor-network theory to study the construction and preservation of networks (Dawson & Jöns, 2018). Actor-network theory was a useful lens to explore the strategies used by leaders to protect information systems from cyber threats because of the ability to represent the heterogeneity of networks and human and nonhuman actors to develop a new systematic process or change.

Operational Definitions

Cyber: The realm of computer network systems under the authority of countries and organizations (Williams, 2014).

Cyberattack: Malicious attacks that consist of disabling computer devices and networks, resulting in the loss of data (Popescu & Popescu, 2018).

Cybercrime: Crimes that involve computer hardware, software, and other technological devices for unlawful purposes, such as deception, stealing, automated sabotage, violation of intellectual properties privileges, and stealing mainframe systems and networks (Lagazio, Sherif, & Cushman, 2014).

Cybersecurity: Tools, policies, security models, security precautions, strategies, risk management tactics, activities, preparation, best practices, guarantee, and

technologies used to protect the cyber atmosphere, institutes, and user data (Reid & Van Niekerk, 2014).

Data breach: A data breach is a deliberate or unpremeditated discharge of protected or private data to an untrusted venue (Sen & Borle, 2015).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are presumptions assumed valid by the researcher that cannot be authenticated (Marshall & Rossman, 2016). The first assumption in this study was that the participants provided honest and truthful answers regarding cybersecurity strategies in their business. The second assumption was that the participants' responses to the interview questions resulted in the collection of rich data for common theme development involving cybersecurity practices at small financial institutions. An authorized official of the financial institution provided access to company documents, and I assumed the documents were accurate and complete.

Limitations

Marshall and Rossman (2016) defined limitations as weaknesses in research. A limitation of this study was that the accuracy of the interview data collected relied on the experience and opinions of leaders in a single financial institution. The sample population being restricted to Doha, Qatar, was also a limitation. Future researchers might transfer the findings of this study to other cases, but because of the narrow scope of the study, limited transferability of the findings exist. A final limitation was my reliance on the

forthrightness of potential participants to identify leaders in the financial industry who implemented successful strategies to protect information systems from cyber threats.

Delimitations

Marshall and Rossman (2016) defined delimitations as the boundaries and scope of a study. A delimitation of this study is the small sample size. The geographical area of the study in Doha, Qatar, was also a delimitation. The triangulation of data collected through interviews and document review may have resulted in the exclusion of useful information I could gain through other qualitative and quantitative designs. Researching through the lens of actor-network theory was a delimitation as well.

Significance of the Study

Business leaders might find value in this study to implement proven strategies to protect information systems from cyber threats, leading to improved business practices and positive social change. The finding might result in a reduced gap in business knowledge regarding cybersecurity practices essential for small financial institutions to avoid potential data breaches. Al-Hamar (2016) recognized that the adoption of information and communication technology intensified in Qatar's cyberspace, which is essential to society, government, and businesses. Al-Hamar acknowledged that pliability and safekeeping in cyberspace are imperative to Qatar's continued achievement and development. A cybersecurity strategy for small financial institutions may guide public expenditures and efforts toward building a more secure business environment.

Contribution to Business Practice

Business leaders in the financial sector might improve business practices by gaining insight into effective strategies used in protecting small financial institutions' information systems from data breaches. Small financial institutions with inadequate budgets for security and data protection remain at risk for cyberattacks. Small financial institutions lack the resources, finances, and security infrastructure that larger organizations employ to prevent or mitigate cyberattacks (Harris & Patten, 2014). Advancing attentiveness is an intentional method of protecting small business data. The execution of cybersecurity strategies has fostered positive economic and social benefits, which have improved local consumer confidence while lessening consumer risk (Federal Bureau of Investigation, 2015). By documenting actual leaders' practices with cybersecurity strategies, the findings of this study might result in business leaders improving their business practices through reductions in cyber threats.

Implications for Social Change

Innovative corporate leaders use technologically advanced digital privacy to implement positive social change, reduce consumers' exposure to security breaches, and improve community engagement (Jewkes & Yar, 2011). To decrease the cost to consumers, business leaders need to recognize the best strategies to reduce data security breaches. Lai, Li, and Hsieh (2012) pointed out that 81% of data security breaches occur because of consumer data theft. Leaders of small financial institutions might improve the protection of consumer data and reduce the costs associated with consumer identity theft by implementing the recommendations from this study. Enlightening business leaders

about ways of thwarting and alleviating cyber threats may aid in business growth and profitability for expanding organizations' support for society (Cant & Wiid, 2013; Coetzee, Preez, & Smale, 2013). Small financial institutions can minimize the exposure of their network systems from cyberattacks with the creation of cybersecurity strategies.

A Review of the Professional and Academic Literature

A critical analysis of the literature informed the research for this qualitative, single case study. The purpose of this study was to explore the approach that leaders of small financial institution use to protect information systems from cyber threats. The goal of this study was to add knowledge to reduce the gap in business practice about cybersecurity policies. Business leaders of financial institutions who lack cybersecurity strategies to protect information systems from cyber threats might benefit from this study. I interviewed five business leaders from a small financial institution to reach an understanding of the research problem.

The literature review in this study encompassed peer-reviewed journal articles, seminal books, dissertations, and government reports. Keywords I used during the search for peer-reviewed journal articles were *actor-network theory, complex adaptive systems theory, banking sector, business strategy, strategies or methods or techniques, cybersecurity, financial institution, financial security, strategy, structuration theory, Qatar, structuration theory, information security, business leadership strategies, leadership, policy, information security, management,* and *risk management*. The databases I used in this study were Walden University Library, ABI/INFORM Complete, Academic Search Complete, Business Source Complete, EBSCO eBooks, Emerald

Management, ProQuest Central, SAGE Premier, and ScienceDirect. The sources I used in this study were (a) 299 peer-reviewed articles, (b) nine dissertations, (c) 11 seminal books, and (d) one government source. Of the 320 sources used, 93% were from peer-reviewed scholarly journals and 272 (85%) had publication dates from 2014 to 2019. I used 154 sources in this review of the academic and professional literature. The specific themes that appeared from the literature review were (a) actor-network theory, (b) complex adaptive systems theory, (c) structuration theory, (d) financial business cybersecurity policies, (e) small business cybersecurity policies, (f) successful leadership strategies for cybersecurity policy, (g) financial institutions strategies, and (h) risk management.

Literature Related to Actor-Network Theory

I explored small financial business leaders' strategies to develop cybersecurity policies to protect information systems from cyber threats through the lens of actor-network theory. Actor-network theorists shape firsthand insights into a range of academic subjects beyond science and technology investigations by aiding to understand the beginning and knowledge of entities (Dawson & Jöns, 2018). Actor-network theory research has spanned from science and technology studies to the social sciences and humanities (Sayes, 2017). Actor-network theory has been used, for example, in the study of economics and organizations (Sayes, 2017). Parker (2017) used actor-network theory to explore how phenomena or entities collaborate to form groups or networks of relations and associates. Conversely, Cavalheiro and Joia (2016) postulated that actor-network theory is a simplified approach in information systems literature because of the

conceptualization of technology as one of the human and nonhuman actors in any actor-network analysis.

The tenets of actor-network theory are agnosticism, generalized symmetry, and free associations (Luscombe & Walby, 2017). Agnosticism is the abolition of preconceived notions in the network (Law, 1986). Generalized symmetry is nonhuman actors (e.g., information technology, software, and cybersecurity strategies) and human actors (e.g., business leaders, project team members, and budget analyst) incorporated in the network or framework with the same agency (Callon, 1986). Free association is a concept that Latour (1986) described as between natural and social phenomena; this difference is that the network gave no value.

Actor-network theorists have researched the role of technology in social science settings to explore the effects of technology on social elements (Sayes, 2017; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). Actor-network theory is essential in exploratory affiliations in which actors participated and influenced the shape of the independent networks (Iyamu & Mgudlwa, 2018). Actor-network scientists have outlined how actors developed groupings and enrolled additional actors by using nonhuman actors to reinforce these relations and their benefits (Tsohou et al., 2015). Researchers have used actor-network theory to explain how individuals make parallel their interests in technological components (Tsohou et al., 2015). Business practitioners have used actor-network theory to gain insight into the conciliations that take place among stakeholders when introducing a technology-driven change strategy (Tsohou et al., 2015). Actor-network theorists have analyzed the way people and technological artifacts establish

sociotechnical relationships to implement change (Tsohou et al., 2015). Dawson and Jöns (2018) mentioned that actor-network theorists draw attention to how material objects, sources, and infrastructure shaped human connections and added to the equilibrium of social structures and the guiding of human practices.

Social scientists have associated actor-network theory with the equal treatment of human and nonhuman actors. Dawson and Jöns (2018) noted that in using actor-network theory's generalized principle of symmetry, human and nonhuman actors were treated equally when analyzing how networks formed, how social relationships even out, and how new actants developed and how their power associations change. Actants are human and nonhuman actors in a system that take the form they do by their relationships with one another (Darnell, Giulianotti, Howe, & Collison, 2018). Scholars have assumed that all entities in a system could and should be described in the same terms (Dawson & Jöns, 2018; Hopkinson, 2017). Ahmed Shareef, Hughes, and Petridis (2014) used actor-network theory to explore the contribution of nonhuman actors to strategies used by leaders in developing cybersecurity strategies in small financial institutions. Lee, Harindranath, Oh, and Kim (2015) used actor-network theory as an interpretive lens to analyze processes. Lee et al. (2015) used actor-network theory to explain how actors configuration associations and join other actors, incorporating nonhuman actors to secure their interests.

Iskandarova (2017) noted that actor-network theory provided insight into the complexity of the policy network. Theorists' arguments informed several case studies in which information systems were explored as actor-networks inhabited by humans and

nonhumans (Müller & Schurr, 2016). Pieters (2011) investigated the relation between explanation and trust in the context of computing science using actor-network theory. Modell, Vinnari, and Lukka (2017) noted the philosophical and practical compatibility of actor-network theory and interventionist research and searched for explanations for their limited joint use. Conversely, Balzacq and Cavelty (2016) postulated that some cybersecurity experts used the core tenets of actor-network theory for a better understanding of what the stakes of cybersecurity are and how information systems work and fail. In agreement with Balzacq and Cavelty (2016), Sadoway and Gopakumar (2017) commented that actor-network theory focused on sociomaterial, political, and spatial implication of urban infrastructure bunding practices.

Scholars have used actor-network theory for commitment, communication, transparency, and trust to satisfy the relationship between information technology leaders and organizations, reducing obstacles in project team relationships (Mendez, Castillo, Sanchez, Mateus, & Maldonado, 2014; Shahin, Jamkhaneh, & Cheryani, 2014). Kurokawa, Schweber, and Hughes (2017) applied actor-network theory to examine how an individual's performance guided, continued and stopped during information technology practices in a central management enterprise. For example, Montenegro and Bulgacov (2015) discovered that networks affect social interaction, financial systems, and political climates, and this contributes to the sustainability of the information technology industry. Iyamu and Mgudlwa (2018) acknowledged the strengths and weaknesses of an information technology leader network and proposed to take full advantage of the capabilities of the system using actor-network theory.

Social scientists have used actor-network theory to locate different types of parts in a network to recognize how those parts shaped and defined each other (Parker, 2017). For example, Kurokawa et al. (2017) conducted a study using actor-network theory's concepts of problematization, enrollment, and durability to study client engagement. Kurokawa et al. moved the conversation of client engagement past the regular call for improved amalgamation to the attentiveness of the mechanisms by which clients engaged. Dumay and Rooney (2016) noted that actor-network theorists focus on linking meaning with substances and procedures, which is beneficial when considering how actors affect the successful application of technology change. In agreement with Dumay and Rooney, Bowers (2018) commented that actor-network theory made observable the variety of actors and connections that worked to create social orders and practices that attempt to standardize regained remediated landscapes.

Researchers have used actor-network theory in research about information systems. Bowers (2018) noted that actor-network theory is a group of philosophies established both in theoretical and empirical research that allocated the principle of the inseparability of social and technological elements. Balzacq and Cavelty (2016), in accord with Bowers, commented that actor-network researchers achieved distinction in international relations and security because of the innovative types of issues and research questions brought on by the material turn. Material turn, defined as an interest in the important of artefacts, natural forces, and material regimes in social practice and systems of powers, as well as the practice turn, which yields structured procedures of doing and saying procedures as the smallest unit of inquiry rather than actors or assemblies

(Balzacq & Cavelty, 2016). Adding to Balzacq and Cavelty, Cavalheiro and Joia (2016) and Parker (2017) mentioned that actor-network theory is significant in information systems literature.

Practitioners have used actor-network theory in economic research. Shim and Shin (2016) applied the lens of actor-network theory to direct a multilevel examination of past progress of China's financial technology sector. Shim and Shin sought to elucidate the development of the building and interrupting an assortment of networks comprised of varied actors implicated in the appeared convergence industry. Gårseth-Nesbakk and Kjærland (2016), building on the work of Shim and Shin, used actor-network theory to study the efforts of eight municipalities to recuperate money in the wake of financial losses from a fiscal crisis. The findings from Gårseth-Nesbakk and Kjærland's research indicated punctualization is costly when dealing with risky investments and participating in blame gaming, as simplifications might suggest unfavorable effects. In agreement with the use of actor-network theory, Adaba and Ayoung (2017) conducted an exploratory cross-sectional field study at three sites in the Upper East region of Ghana to understand the gradual decrease of the infringement and dispersal of mobile money service.

Practitioners have discussed the use of actor-network theory in cybercrimes. Luppicini (2014) conducted a review of literature from 2002 to 2013 that connected research studies at the crossroads of actor-network theory and cybercrime and addressed the following question: How does actor-network theory apply to cybercrime research? Van Der Wagen and Pieters (2015) noted that actor-network theory gave a stable viewpoint on the human and nonhuman agency in amalgam cybercriminal networks, and

they explored a botnet case from this perspective. In comparison, Eze and Chinedu-Eze (2018) examined how small and medium enterprises are immersed in developing information and communication technology implementation by focusing on the adoption method and the role played by numerous actors in the procedure through the lens of actor-network theory. Conversely, Modell et al. (2017) examined the potentials and trials of merging process concepts in accounting research through an exploration of research papers with connection insights from institutional theory and actor-network theory. Gunawong and Gao (2017) investigated the underlying process-based causes of government failure through the lens of actor-network theory.

Luppicini (2014) noted the advancement of awareness at the junction of actor-network theory and the research of cyber criminology. Van Der Wagen and Pieters (2015) agreed with Luppicini that actor-network theory is suitable for understanding on the amalgam and interlinked offending, victimization, and defending activities, leading to the new conception of cyborg crime. Modell et al. (2017) postulated that accounting researchers should carry out reflexivity regarding the typical insinuations of merging method theories and the overall justifiability of such practices as a vehicle for progressing the understanding of accounting as a social and organizational procedure.

Eze and Chinedu-Eze (2018) provided value to practitioners and academics, as they offered insight into the information and communication technology outline by showing how the various actors guarantee emerging information communication technology adoption in small service businesses. Zawawi (2018) used actor-network theory to investigate the effects of interorganizational management control systems on an

organization and found that the dynamics of interorganizational units and management control systems are explainable from an actor-network perspective. De Albuquerque and Christ (2015) investigated the outcomes of process modeling on the flexibility of small businesses through the lens of actor-network theory. De Albuquerque and Christ used actor-network theory to describe a multidimensional comprehension of flexibility as a relational influence of sociomaterial networks.

Complementary and Alternative Theories

Complex adaptive systems theory and structuration theory were possible conceptual frameworks for this study. Actor-network, complex adaptive systems, and structuration theories include some aspects of human and nonhuman actors relating to policy and process development in the area of information systems. For this study, I explored the limitations of the complex adaptive systems theory and structuration theory.

Complex adaptive systems theory. Complex adaptive systems theory originated in the natural sciences to articulate how interacting agents such as organisms adapt and coevolve over time in logical ways (Srinivasan & Mukherjee, 2018). Complex adaptive system theorists have described evolutionary change procedures, postulating understanding into how the beginnings of quality assurance centered on reasonable linearity and reductionism (Malik & Pretorius, 2018). A complex adaptive system is a sophisticated macroscopic gathering of relatively alike associated microstructures shaped to acclimatize to an altering setting (Van Brussel, Boelens, & Lauwers, 2016). In agreement with Malik and Pretorius (2018), Reid (2016) stated dynamic networks of

associations and connections, not accumulations of static objects, as complex adaptive systems.

Scholars have considered an entity or concept as a system when deciphering complexities (Christo, Dewald, & Emmanuel, 2016). Expressly, researchers have noted that understanding humans and their environment is part of an interacting system from a system science approach (Christo et al., 2016). Christo et al. (2016) stated that complex adaptive system created a means of trying to understand inherently nonlinear systems, such as economies and behavior of cybercriminals, which are hard to imitate using linear analytical tools such as mainframes. In agreement with Christo et al., Fidan (2017) commented that complex adaptive systems theory is a structure for explicating the appearance of system level (i.e., cybersecurity process) order ascending from the collaboration of the system's symbiotic agents (i.e., people, departments, ideas, information, resources); thus, using complex adaptive systems theory, Fidan concentrated on the interplay between a network and environment. Conversely, Akgun, Keskin, and Byrne (2014) commented that complex adaptive systems theory is an emerging research area in the new product development literature, which gave a framework for explaining the emergence of system-level order arising from the interactions of systems' interdependent agents.

Complex adaptive systems theorists in management and social context view organizations as actors with the essential capability to deal with change, interacting with each other and with the business environment (Srinivasan & Mukherjee, 2018). Investigators have interpreted information systems emergence using complexity concepts

(Srinivasan & Mukherjee, 2018). Christo et al. (2016) conceptualized the tenets of a complex adaptive system as understanding complex emergent behavior at a large-scale level by looking at exchanges between inhomogeneous parts at a micro level. Additionally, Christo et al. characterized complex adaptive systems with the ability to learn from the environment. Finally, Christo et al. asserted that the learning aimed to bring about modification or alteration to the system that facilitates survived or absorbed shocks to the system. Equally, Ghazzawi, Kuziemsky, and O'Sullivan (2016) noted that feedback, emergent behaviors, nonlinear processes, coevolution, requisite variety, and simple rules are tenets of complex adaptive systems. Accordingly, involved adaptive system researchers can be said to be fundamentally characterized by anarchy, or the ability to be animatedly influenced or adjust to changes that emerged within or outside a system (Ramos-Villagrasa, Marques-Quinteiro, Navarro, & Rico, 2017).

Scholars used actor-network theory and complex adaptive systems theory in conjunction with information systems management and research (Afzaal & Zafar, 2016; Ghazzawi et al., 2016; Van Brussel et al., 2016). Afzaal and Zafar (2016) explained complex adaptive systems as agents and individuals of dynamic networks that behave in equivalence and continuously respond to each other. Van Brussel et al. (2016) noted that social scientist remained concerned with the intentionality and enactment of individual actors. Conversely, Fidan and Balci (2017) pointed out that complex adaptive systems optimal performance occurred when the actors work as an interrelated network of dependent components. Ghazzawi et al. (2016), in agreement with Afzaal and Zafar, commented that complex adaptive systems are a problem-solving approach that

acknowledged the complexity of organizations and networks and the relationships within and between system components.

Scholars have defined complex adaptive systems in many ways. Marjanovic and Cecez-Kecmanovic (2017) expounded complex adaptive systems act together and trade information within the environment in a conjointly modeling behavior in open network systems. Van Brussel et al. (2016) explained how actors interpret the choice systems within environments and change strategies to pursue. Barasa, Molyneux, English, and Cleary (2017), building on the work of Van Brussel et al. (2016) sees small business systems as many interrelated parts with humans and nonhumans whose exchanges and procedures are dynamic, instantaneously affecting and influencing the system. Conversely, a scholar explained actor-network prevail over complex adaptive systems theory state-based analysis by highlighting how the transition between states, or other landscapes (Van Brussel et al., 2016).

Structuration theory. The structuration theory is a theory of the formation and imitation of social systems that build on the investigation of together structure and agents, without providing importance to either (McGarry, 2016). In structuration theory, neither macro- nor micro-focused investigation alone is enough (McGarry, 2016). Giddens created the structuration theory, most knowingly in *The Constitution of Society*, which examined phenomenology, hermeneutics, and social practices at the attached connection of agent and structures (McGarry, 2016). Structuration theorists found structure as resources and rules, recursively associated with the imitation of social systems (Sergeeva, Huysman, Soekijad, & van den Hooff, 2017). By posting structure as resources and rules,

Giddens suggested that any act by human agents involved power (Dutta, Malhotra, & Zhu, 2016). Individually, agents evaluated forms of structures when making decisions: structures of signification or institutionalized explanatory arrangements such as values and beliefs assigning meaning to people's action; structures of legitimation or standardized norms, expressed as moral imperatives and normative sanctions; and structures of supremacy or institutionalized mobilization of power, signified as to how resources are allotted, retrieved, and employed (Dutta et al., 2016). With the use of structuration theory, human relations draw on socials' structures and at the same time produces, reproduces, or changes these structures (Tsohou et al., 2015). Social systems are structural properties, which researchers and practitioners use to explain like social practices over space and time (Tsohou et al., 2015).

Scholars studied cybersecurity and information security through the lens of the structuration theory. In a qualitative case study, Nasution, Dhillon, and Akyuwen (2017) investigated how security policies formed in organizations, traditional, and therefore, prevent security breaches in the Indonesian banking sector. The result of the study was a source of a theoretical model to formulate and implement security policies in a commercial bank (Nasution et al., 2017). Conversely, Tsohou et al. (2015) commented that interrelated changes, such as security awareness processes, occurred at the organizational, technological, and individual level. Tsohou et al. introduced an integrated analytical scaffold created through action study in a public sector organization, comprising actor-network theory, contextualism, and structuration theory. Tsohou et al. illustrated the limitations of each theory to study multilevel modifications when used

individually, established the cooperation of the three theories, and proposed how the theories can be used to research and manage awareness related changes at the individual, technological, and organizational level.

In contrast with Tsohou et al. (2015), Michael and Tiko (2015) noted the effect of organizational polities on information technology strategy formulation and implementation in an organization using the structuration theory. Michael and Tiko considered the interplay between stakeholders in influencing information technology strategy formulation and implementation in an organization as a socially constructed phenomenon. Thus, Michael and Tiko interpreted and understood the event by using social theories, such as structuration theory. Michael and Tiko adopted actor-network theory as a lens through which to understand and interpret the sociotechnical processes associated with information technology strategy formulation and implementation in an organization. In contrast to Michael and Tiko, Nasution et al. (2017) used Gidden's structuration theory to explore how information security policies and practices are shaped and assimilated in an organization.

Financial Business Cybersecurity Policies

Leaders of financial institutions must adapt to the increasing frequency and diversity of cyberattacks (Coole & Brooks, 2014; Kshetri & Voas, 2017). Nastasiu (2016) pointed out that leaders use cybersecurity strategies to identify the risks and threats, determine the course of action in case of a cyberattack, and outline the steps to follow to minimize the effects and catch the perpetrator. Social scientists pointed out that financial firms need information security policies and procedures to support the decision making

the process of management to reduce the risk of cyber threats (McGarry, 2016). Gallagher, McMahon, and Morrow (2014) commented that the average number of cyberattacks on financial organizations increased by 169% between 2012 and 2013. Jackson, Saffell, and Fitzpatrick (2016) noted that emerging technologies and the increasing sophistication of threats are the top reasons that leaders of financial firms face difficulties in implementing cybersecurity measures. Financial institutions are the primary targets of cyberattacks. Banks are depositories for cash, and for cybercriminals, attacking banks offers multiple avenues for profit through extortion, theft, and fraud, while nation-states and hacktivist also targeted the financial sector for political and ideological advantage (Ananda Kumar, Pandey, & Punia, 2014). Regulators took notice and implemented new security policies for cyber breaches that addressed the growth to the banks they supervise (Ananda Kumar et al., 2014; Dang-Pham, Pittayachawan, & Bruno, 2016).

Cyber concerns in the banking sector were a business issue in the early era of banks using electronic transaction and network capabilities (Farzan et al., 2013). Scholars conducted studies for forming robust information technology security strategies. One of the concerns of most financial leaders was the cost of data security upgrades because the return on the investment on security was difficult to predict and govern (Gai, Qiu, & Sun, 2018). Terlizzi, Meirelles, and Viegas Cortez da Cunha (2017) noted that to mitigate the risk of a collapse in the global financial system caused by a succession of successful cyberattacks, regulators suggested that financial organizations integrate a cybersecurity framework in their information technology governance processes. Servidio and Taylor

(2015), in agreement with Terlizzi et al., commented that the first step in establishing a cybersecurity program for a community back is to adopt and adhere to a series of formal, written procedures and policies, which will be the foundation of the bank's cybersecurity risk governance framework. Stanciu and Tinca (2017) pointed out that to approach the risk of cybersecurity most appropriately the information security specialist gives precedence to the focus and issues on the most significant ones from the business perspective.

Business leaders studied the laws and regulations needed to mitigate cybercrimes within financial institutions. Mohammed (2015) investigated statutes and rules in the commercial business sector applicable to cybersecurity. Lagazio et al. (2014) studied the consequences of Internet attacks on the financial industry. Damghanian, Zarei, and Siahsarani Kojuri (2016) examined the affiliation between clear security and acceptance of online banking with the interceding consequence of real risk and trust in Internet financial transactions in Iranian customers. Mohammed noted compliance and regulatory issues across the financial industry on a state and federal level.

In comparison to Mohammed (2015), Lagazio et al. (2014) showed vulnerabilities in the strategic behavior of financial companies, for instance, gradually expenses on defense and tenacious under-reporting of cybercrime occurrences. Conversely, Damghanian et al. (2016) commented that the variables of perceived security and trust in Internet banking had a positive effect on the acceptance of online banking. Mohammed uncovered the operational differences and repercussion in cybersecurity resulted from shared requirements from the Gramm-Leach-Bliley, Sarbanes-Oxley, and Dodd-Frank

Acts on small and large financial institutions. The findings from Damghanian et al.'s study indicated that perceived risk had a significantly adverse effect on confidence in Internet banking.

Leaders of financial institutions developed policies to improve the efficiency of the institution. Comizio, Dayanim, and Bain (2016) provided financial firms with an outline of the changes in cybersecurity protocols of financial establishments throughout the United States, the United Kingdom, and the European Union. Comizio et al. presented advice with emerging cyber risk management plans considering growing cyber threats and cyber governing anticipations. Comizio et al. discovered cyber risks, and financial watchdogs' expectancies for cybersecurity evolved, noting the need for leaders of financial institutions to advance cybersecurity protocols. Sipes, James, and Zetoony (2016) provided an approach for financial services firms to design some significant procedures and policies associated to cybersecurity programs, which comprised of document retention strategies, making incident response plans, and beginning or assessing a bounty program. The information is valued to financial services firms, which faced possible financial implications and growing regulatory ramifications, which included enforcement fines, penalties, and actions, for the failure to implement a cybersecurity program (Sipes et al., 2016).

Cyber risk is the most critical risk area affecting financial institutions (Blank, Kohlhofer, & Bonaccorsi, 2016; Giblin, 2015; Netkachova & Bloomfield, 2016). Camillo (2017) acknowledged that the majority of cyberattacks against global financial institutions remain unreported. Lemieux (2015) estimated, in 2013, 21 % of commercial

bank accounts were the object of a takeover by cybercriminals, with 9 % resulting in funds leaving the institution. Kim (2017) reported that the United Kingdom government acknowledged that a cyberattack infected two-thirds of the country's larger businesses within the previous 12 months. Leaders of financial institutions need to embark on a whole risk management strategy to combat the renewed threat of ensuring that a tripartite approach that embraced rigorous internal procedures, the adoption of external professional support and the use of proper insurance cover is in place (Camillo, 2017).

For business leaders, a central responsibility is to ensure that the institutions maintain written policies and procedures related to cybersecurity (Blank et al., 2016; Herath et al., 2014). To mitigate the risk of a collapse in the global financial system caused by a succession of successful cyberattacks, regulators indicated that financial organizations integrate a cybersecurity framework in their information technology governance process (Terlizzi et al., 2017). Although a cybersecurity framework is a set of industry best practices and standards leaders used to aid cybersecurity risks and defend digital assets from adversaries, information technology governance consists of information technology leadership and procedures to ensure compliance with an enterprise's principles (Terlizzi et al., 2017). Stechyshyn (2015) conducted research to propose the implementation of a security system engineering discipline by financial institutions. Stechyshyn noted that leaders of financial institutions must comply with the requirements of the Federal Financial Institutions Examination Council. Tabassum, Mustafa, and Maadeed (2018) explored the effects of cybercrime to understand the force of damage caused to businesses. Tabassum et al. used Qatar as a case study emphasizing

the difficulty of securing cyberspace. Tabassum et al. noted the need for a global response to curb cybercrime. Past cyberattacks in Qatar caused leaders to increase consciousness and start actions for improving cybersecurity (Tabassum et al., 2018). Abdul-Wahab and Haron (2017) conducted an empirical investigation collecting data from 15 Islamic conventional and foreign banks that examined the efficiency of the banking sector in Qatar. The results from their study indicated that Qatari banks operate below optimum performance (Abdul-Wahab & Haron, 2017). Abdul-Wahab and Haron noted that all the Qatari banks experienced a decrease in productivity because of a lack of technological innovation in the banking segment of Qatar.

Small Business Cybersecurity Policies

Cybersecurity is critical for businesses of all sizes. Patrascu (2018) pointed out that the United States first developed a cybersecurity strategy in 2013. Mansfield-Devine (2016) noted that small businesses are at the same risk for cyberattacks as larger companies. Ahmad, Maynard, and Park (2012) pointed out that organizational leaders must develop information security strategies using a standard framework for the expansion, institutionalization, valuation, and enhancement of an information security policy to discuss information security risks.

Paulsen (2016) commented that the adaptability advantages small businesses have over larger institutions could change the delicacies of the cybersecurity landscape and make them leaders in the field if small companies collectively embrace cybersecurity. Gao and Zhong (2015) investigated information security investment tactics for both mass and targeted attacks by considering calculated dealings between two rival firms and a

hacker. Iverson and Terry (2018), in agreement with Gao and Zhong, noted security awareness education is an effective method of keeping companies secure from cyberattacks. Conversely, Gordon, Loeb, Lucyshyn, and Zhou (2015) evaluated the influence of government motivations intended to counterbalance the propensity to underinvest in cybersecurity-associated events by small businesses using the economics based analytical framework. Gordon et al. showed the possibility for government motivations or guidelines to enlarge cybersecurity funds by small companies is reliant on two fundamental issues: small businesses used the best mixture of contributions to cybersecurity and small organizations willingness to increase resources into cybersecurity strategies. Gao and Zhong showed that security requirements altered the contrasts of investing approaches under the two types of cyberattacks. Gordon et al. provided a conversation of activities by the U.S. federal government that used beforehand, or in combination through, contemplating new government motivations or regulations for cumulative cybersecurity capital spending by small businesses. On the contrary, Gao and Zhong proved that company leaders preferred to control security measures when the degree of rivalry became aggressive but choose relaxed security measures when the degree of competition was minor. In support of Paulsen (2016), Iverson and Terry (2018) posited that having a comprehension of the organization's risks and a plan surrounding the security tactics can assist small businesses on the path toward better information technology data security and sustained business success.

Business leaders studied operational efficiencies with information systems security. For example, Trim and Lee (2010) conducted a study that focused on managers'

allocated framework for minimizing cybersecurity vulnerabilities through network defense tactics. Trim and Lee paid attention to how senior executives created strategies that combined counterintelligence and sited risk in a controllable context. Trim and Lee's findings indicated that for senior executives to cut the threat from cyberattacks, management needed to create relationships with third-party organizations and government representatives. Hall, Sarkani, and Mazzuchi (2011) researched the association between organization performance and information security strategies, with organizational competencies as factors that influenced the implementation of organizational performance and information security strategy. Hall et al. found organizational abilities encompassed through the aptitude to change superior situational alertness of current and future risk atmosphere, ability to have proper methods and volume to arrange the processes to react to data security intimidations, are positive effects on organization performance. Hall et al. noted that no relationship existed amid judgment making and the data security policy execution process. Hall et al.'s findings yielded applied worth for professional leaders to understand the realistic tendency of organizational proficiencies in the framework of information security, therefore allowing businesses to center on attaining the ones essential for educating organization routine.

Successful Leadership Strategies for Cybersecurity Policy

The literature review explained that business and security strategies are essential in the decision-making process of senior leadership (James, 2018). James (2018) pointed out that 95 % of business leaders recognized cybersecurity as being an area of high significance, but 45 % had no formal stratagem in place. Schneider (2018) explained that

80 % of small firms lack a cybersecurity policy. Organizational leaders should reconsider methods to cybersecurity to protect shareholder benefits and evade regulatory sanctions (James, 2018). To counter the evolving cyber threat facing organizations, business leaders must ensure they have an integrated approach to cybersecurity tailored to their business and risk profile, focusing not only the technical aspects of their defense but also the people and organizational elements (McGarry, 2016).

Scholars pointed out the best strategies for cybersecurity in literature. Fakhri, Fahimah, and Ibrahim (2015) explained that business leaders should align operational enterprise systems with security practices through embedding information security risk management into the organization. Business leaders must understand the strategic implications of a cyberattack to overcome an attack on their information systems (Copeland, 2017). For the Internet to be an open and global podium, business leaders will have to come from various stakeholders being an internationally different set of perspectives an interest, prearranged in new and creative ways rather than along the conventional lines of stakeholder groups (Sepulveda, 2017). Conversely, Bell (2017) pointed out that the foundation of a resolution to prevent and mitigate cyberattacks needed a cooperative, hands-on association premised on information sharing between the private and government sector.

Business leaders should deal with potential components' vulnerabilities, improve communication security in the network, and defend customer privacy. According to Selznick and Lamacchia (2018), because of the limited resources and technological skills, small businesses are easy prey for hackers. Watad, Washah, and Perez (2018), in concert

with Selznick and Lamacchia, commented that small business leaders should realize that information technology security is a necessity and a cost of conducting business. Conversely, Mrabet, Kaabouch, Ghazi, and Ghazi (2018) proposed a cybersecurity strategy composed of three levels: pre-attack, under attack, and post-attack. Business leaders acknowledge the importance of leadership in cybersecurity policy development. The quintessential to security governance procedures is to have a robust internal leader, often a chief information security officer, who collaborated with legal experts to guide the organization before, during, and after a crisis (Karanja, 2017). The senior management teams and human resource handle cybersecurity strategies within the organization (Karanja, 2017). Human resources managers can help by working with the cybersecurity team, the entire corporate level management suite, and the board to create, communicate and cascade rules and protocols to keep the enterprise safe (Karanja, 2017). To support Karanja (2017), Lowry and Moody (2015) noted that a lack of conformity with information security strategies is a prevalent organizational matter that bears excessively large direct and qualitative costs that undermined stratagem. The exercise of leadership desired a readiness on the part of policymakers to engage interested parties within their jurisdictions and abroad in the detection of solutions in good faith, from connecting everyone in the world to confirming the safe and useful of connectivity (Sepulveda, 2017). Conversely, Safa, Maple, Watson, and Von Solms (2018) suggested that management should pay notice to the environmental factors that inspire employees to engage in information security misconduct.

Financial institutions strategies. Cybercrime is one of the most common types of economic crime reported by financial services (Senol, 2017). Financial institutions embarked on a holistic risk management strategy if they are to combat the renewed threat effectively (Camillo, 2017). The increase of cyberattacks and regulatory cybersecurity requirements, combined with the limited resources of smaller institutions, created an opportunity for such institutions to remediate threats (Korte, 2017) proactively. Continuous investment in current technologies and security measures helped prevented financial, and information loses triggered by cyberattacks on financial organizations (Mbelli & Dwolatzky, 2016). Bank leaders redefined their security management systems by nonstop supervising approaches to have a complete view and information of threats on a day-to-day basis (Mawudor, Kim, & Park, 2015). Low-cost strategies to strengthen cybersecurity in financial institutions include giving employee education and training, checking social media, and enhancing password protection (Anderson, 2017). Anderson (2017) noted other strategies, such as setting up a cybersecurity program and performing risk assessments. To combat cyberattacks, banks leaders pursued a complete and top-down tactic to cybersecurity in banks. Cybersecurity needs to be an inventiveness commanded by senior leadership, not just assigned to the chief information security officer (Patrascu, 2018). Meeting regulatory expectations is a large part of financial institutions' cybersecurity strategies (Štitilis, Pakutinskas, Kinis, & Malinauskaitė, 2016). Business leaders of financial institutions must broaden their focus from improving processes to integrating risk management, compliance, and ethics into their organizations' culture (Štitilis et al., 2016). In agreement with Camillo (2017), Rothrock,

Kaplan, and Van (2018) mentioned that asking the right question is a strategy to address cybersecurity risk management in organizations.

Cybersecurity risk management. Risk management is a principle of cybersecurity (Burley, 2018). Risk management is the identification, evaluation, prioritization, minimization, and control of risks (Höring, Gründl, & Schlütter, 2016). Risk management aims to ensure that ambiguity does not deflect the endeavor from the business goals (Yang, Hsu, Sarker, & Lee, 2017). Practitioners acknowledged risk management as an essential aspect of developing cybersecurity strategies in financial institutions (Banham, 2017; Camillo, 2017). Shires (2018) proposed that cybersecurity ability is a skilled performance, which assures decision makers' calls for risk management.

Corporate governance is the foundation of effective risk management in the bank, and thus, the foundation for a sound financial system (Ananthasubramanian, 2018). Meszaros and Buchalcevova (2017) proposed a scaffold for online services security risk management used by both service providers and customers through a case study approach. Alali, Almogren, Hassan, Rassan, and Bhuiyan (2018) proposed to apply the fuzzy inference model to create risk evaluation results based on the four risk factors, which are vulnerability, likelihood, that, and effect to identify the range of risks that can intimidate any entity and attempt to resolve such issues to proposed objects. Conversely, Sheedy, Griffin, and Barbour (2017) suggested a multilevel scaffold for investigating risk climate (the communal feelings among employees of the comparative priority given to risk management, comprising perceptions of the risk associated practices and behaviors

that are expected, valued, and supported), together with outcomes and antecedents, and authenticate an original measure.

Fielder, König, Panaousis, Schauer, and Rass (2018) acknowledged the importance of cybersecurity risk assessment is to undertake uncertainties in risk assessment that affect cybersecurity investments. Griggs and Gul (2017) discussed how New York State enacted cybersecurity regulations to protect the state's financial services industry and consumers from the threat of cyberattacks. The rules included:

- Governance framework controls included requirements for a funded and staffed cybersecurity program managed by qualified management, with periodic reporting to the organization's highest governing body;
- Risk-based standards for technology systems included access controls, data protection including encryption, and penetration testing;
- Needed criteria addressing cyber breaches included an incident response plan, preservation of data to respond to such violations and notice to regulators of material events; and
- Accountability by identification and documentation of material deficiencies, remediation plans, and annual certifications of regulatory compliance to regulators (Griggs & Gul, 2017).

Because of the increased number and evolving nature of cyberattacks, preventing, or cutting all risk of an attack is not a reasonable goal (Griggs & Gul, 2017). Plan sponsors and fiduciaries instead focused on developing an appropriate and proportional response to the risk of a cybersecurity breach of plan data (Griggs & Gul, 2017). Prudent

plan sponsors and fiduciaries developed a cybersecurity risk management strategy proper for the institutions help plans. Conversely, Gonzalez-Granadillo et al. (2018) said proper response stratagems against new and ongoing cyberattacks must decrease risks down to satisfactory levels, without surrendering a mission for security. Gonzalez-Granadillo et al. proposed a dynamic risk management response system consisting of a proactive and reactive management software aiming at evaluating threat scenarios in an automated manner, as well as expecting the occurrence of potential attacks.

Transition

A cybersecurity strategy for leaders of small financial institutions might be useful as a guide for public expenditures and efforts toward building a more secure business environment. Business practitioners noted that inadequate cybersecurity policies make small businesses targets of cyberattacks (Selznick & Lamacchia, 2018). Phishing attacks targeting small business reached 43%, which increased 9% over reported attacks in 2014, and 25% increase in contrast to 2011 (Watad et al., 2018). Small financial institutions with inadequate security budgets and data protection remain at risk for cyberattacks. The purpose of the literature review was to explore the approach some leaders of small financial institution use to protect information systems from cyber threats. A goal of this study is to add knowledge to the gap in business practices regarding cybersecurity policies. The specific themes that appeared from this literature review included actor-network theory, complex adaptive systems theory, structuration theory, financial business cybersecurity policies, small business cybersecurity policies, successful leadership strategies for cybersecurity policy, financial institutions strategies, and risk management.

Section 1 of this study included an introduction to the foundation for the study relevant to the problem and purpose statements, research question, conceptual framework, operational terms, the significance of the study, and review of the literature. In Section 2, a discussion ensues regarding the role of the researcher, the justification for the use of the qualitative method and case study design, and an explanation of the eligibility criteria for participants. I will explain the procedures used to ensure keeping ethical research standards, collecting rich data, conducting data analysis, providing credible, dependable findings, and reaching data saturation. Section 3 will contain the presentation of the findings, conclusions of the research, applications to professional practice, implications for social change, recommendations for action, recommendations for further study, reflections, and a concluding statement.

Section 2: The Project

The focus of this qualitative single case study was to explore small financial institution leaders' strategies to protect information systems from cyber threats. I collected the data in this study from leaders of a small financial institution using semistructured interviews and a review of company documents. In Section 2, I restate the purpose of the study and discuss the role of the researcher, research participants, research method and design, population and sampling, ethical research, data collection instruments, techniques, organization, and analysis. I conclude with a section about dependability, credibility, and confirmability.

Purpose Statement

The purpose of this qualitative single case study was to explore the strategies that some leaders of a small financial institution use to protect information systems from cyber threats. The target population consisted of business leaders from a small financial institution in Doha, Qatar, because they successfully implemented strategies to protect information systems from cyber threats. The implications for social change include the potential for business leaders to reduce data breaches, safeguard the confidential information of consumers, and reduce the risks and costs of consumer identity theft.

Role of the Researcher

I was the primary instrument of data collection for this study. Researchers are the primary tool for data collection in qualitative research (Leedy & Ormrod, 2015). Berger (2015) pointed out that qualitative researchers develop a personal relationship and indulgent connection with the study subject matter when immersed in all components of

the research. The role of the researcher is to collect data using a variety of means to report on the target phenomenon (Ogden & Cornwell, 2010; Wisdom, Cavaleri, Onwuegbuzie, & Green, 2012). As the investigator, I had control of the data collection process.

My role as the chief executive officer (CEO) of a business development company is to bring investors to business entities in Doha, Qatar. I am a decision-maker for the organization, and I develop strategic planning for organizational decisions. I have never worked in the financial business sector. To remove any conflict of interest, I selected participants I had no past or existing professional relationship with. Researchers mitigate bias by selecting participants with whom no professional relationship exists (Balzacq, 2014; Kache & Seuring, 2014; Ülle, 2014). I knew about strategy development and implementation, but not about information systems and cybersecurity in the financial sector, thus mitigating bias in this study.

I kept full control of the interview process. I used semistructured interviews to collect data from participants using an interview protocol (see Appendix A). Yin (2018) pointed out that researchers use semistructured interviews to keep control and elasticity in the data collection process. I obtained informed consent from the participants before the interview. The consent form included an outline of the policies and procedures of the research process. I ensured that participants recognized the risks and benefits of participation before beginning the interviews. Cummings, Zagrodney, and Day (2015) noted that researchers must notify participants of the potential risks of participating in a research study. I reviewed the Belmont Report, a summary of the ethical principles and

guidelines for the protection of human subjects in research (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). Using the Belmont Report protocol—including participant confidentiality, informed consent, and data storage—I addressed the researcher's accountability to discuss ethical concerns. The Belmont Report is intended to protect research subjects who are not knowledgeable about making sovereign decisions (Fiske & Hauser, 2014) . To follow this intention, I completed the Protecting Human Research Participants training offered by the National Institutes of Health Office of Extramural Research (Certification Number: 445524). Resnik, Miller, Kwok, Engel, and Sandler (2015) noted that the participant protection training process can aid researchers in the informed consent process, in the protection of participants, and in dealing with ethical challenges in research.

I placed aside my personal bias to mitigate any risk. Moustakas (1994) described epoché as the process of setting aside prejudgments in a study to eliminate bias. The purpose of epoché is for researchers to set aside prejudices and preferences to ensure that the investigation is pure (Bazzano, 2014). Bias may occur in any study and may cause a researcher to misrepresent the evaluation of information. Brayda and Boyce (2014) commented that researchers who inject their individual opinions or worldviews into a study create the potential for biased results. I reduced systematic research errors and bias by following the qualitative research design and using professional experiential knowledge to review the collected interview responses. Gargon et al. (2014) suggested that careful research design can mitigate researcher bias. During the interviews, I

remained objective and neutral to avoid injecting my opinion or worldview into the data collection process.

I asked open-ended questions during the semistructured interviews with participants. Researchers use a case study process to collect reliable information (Yin, 2018). Bölte (2014) noted that using interviews in qualitative research offered a more in-depth understanding of a researcher's topic. I employed an interview protocol (see Appendix A) as a guide for my interview questions and the interview process. Foley and O'Connor (2013) acknowledged that using an interview protocol adds dependability and credibility to a qualitative study. Scholars have noted that the interview protocol should include reminders of what the researcher should do to ensure the intent of the phenomena under investigation; an opening statement as an icebreaker; open-ended, face-to-face interview questioning; notation and clarification of any nonverbal communication; probing questions; and recorded reflective notes throughout the entire interview process (Onwuegbuzie & Byers, 2014; Rowley, 2012; Thomas & Magilvy, 2011). I followed an interview protocol to ensure that I used the same interview questions with each participant, asked all interview questions in the same manner, and covered the same topics in every interview to mitigate bias (see Appendix A). The interview protocol contained language about interview preparation, opening the conversation, obtaining informed consent, conducting the interview, following up with probing questions, theme verification, coding, and recoding reflective notes (see Appendix A).

Participants

Yin (2018) noted that participants must have experience with the phenomenon in qualitative research. Moustakas (1994) suggested the researcher in a qualitative study should find participants who have the knowledge and expertise needed to answer the research question. Participants must be able to supply aspects and perspectives about a phenomenon in qualitative research (Northrup & Shumway, 2014). I identified potential participants who have the prerequisite knowledge to answer the central research question for this study. Using a purposeful approach, I selected five business leaders who met the eligibility criteria for participation. The eligibility criteria for this study were leaders of a small financial institution in Doha, Qatar, who implemented a successful strategy to protect information systems from cyber threats.

I gained access to potential research participants' contact information through publicly available online business directories: the Qatar Online Directory (www.qataronlinedirectory.com/), Qatcom.com (www.qatcom.com/), and ezyQatar (www.ezyqatar.com/). McCormack, Adams, and Anderson (2013) viewed online listings as a secure space for the enlistment of participants because these database types give profile information to help select members who meet the criteria of a study. Ryan (2013) noted that online directories are a cost-effective, efficient, and productive method to enlist participants for a qualitative study. Smith, Wilde, and Brasch (2012) added that the use of the Internet to enlist research participants is widespread, particularly for researchers conducting interviews. Potential participants received an invitation email and an attached informed consent form. The informed consent form contained a description

of the study, along with a request to contact me directly via email. Once I determined participants' willingness to take part in this study, I built a working relationship with the participants.

I developed a working relationship with the participants by purposely connecting with them through email and in person, having continuous communication throughout the research process, and reflecting on my responsibility to the participants as the researcher. Developing a working relationship with participants in a qualitative study is critical for success (Valipoor & Pati, 2016). Trainor and Bouchard (2013) supported that the researcher-participant association is mutual, so each participant contributes something the other needs or desires to shape the researcher's study. Haahr, Norlyk, and Hall (2014) indicated that researcher and participant interaction during an interview effects trust and confidentiality. The researcher should have precise purposes, values, and views when establishing a relationship with the research participants (Haahr et al., 2014).

Research Method and Design

Research Method

Using the qualitative method, I explored the strategies that some leaders of a small financial institution use to protect information systems from cyber threats. Park and Park (2016) noted that the purpose of qualitative research is for a researcher to advance an understanding of a phenomenon through open discourse with participants and gaining insight from participants' knowledge and ability. The strength of qualitative research is theory amplification and theory creation rather than theory analysis (Reinecke, Arnold, & Palazzo, 2016). Singh (2015) acknowledged that qualitative research gained a reputation

in management research because of the growing involvement of organizational leaders and their experience of continuous fluidity. A qualitative researcher must remain objective and neutral, putting aside personal information and skills that might produce biases, suppositions, and difficulties to the exceptional experiences of the participant (Bailey, 2014). I selected the qualitative method for this study to gain insight and knowledge from participants through open dialog during semistructured interviews.

Quantitative researchers explain events by gathering and examining statistical data (McCusker & Gunaydin, 2015). Barnham (2015) noted that researchers conducting quantitative research accentuate impartial dimensions and the mathematical, arithmetical, or statistical analysis of data collected through polls, surveys, or by influencing preexisting statistical numbers using computational procedures. Quantitative researchers focus on collecting statistical and simplifying data across groups of people or explain a phenomenon (Wagner, Hansen, & Kronberger, 2014). I did not test a hypothesis or apply numerical measurements to validate data; therefore, the quantitative method was not suitable for this research.

Mixed-method scientists merge qualitative and quantitative methods to incapacitate the impending limits of a single research method (Sweeney & Goldblatt, 2016). The mixed-method researcher integrates theoretical suppositions and the use of qualitative and quantitative approaches (McKim, 2015). McCusker and Gunaydin (2015) showed that the mixed-method approach is most appropriate for exploration needing a full and in-depth examination of qualitative data and multivariate analysis of quantitative data. The mixed-method approach was not ideal for this study because I did not use a

grouping of qualitative and quantitative data collection and analysis methods to increase the interpretation of my research problem.

Research Design

Researchers conducting a qualitative study should identify an appropriate design, such as a case study, ethnography, or phenomenology (Marshall & Rossman, 2016). After researching the applicability of each design, I selected case study as the most appropriate design to conduct this study. Yin (2018) asserted that scholars conducting a case study explore actions, procedures, or occurrences experienced by research participants during the time of the event. Anderson, Leahy, DelValle, Sherman, and Tansey (2014) stated that a case study is an appropriate design when a researcher seeks to explore a real-world phenomenon in a bounded setting. I selected the case study design because I was exploring a real-world problem in a bounded setting.

An ethnographic researcher explores the culture of an organization or group of people within the organization or culture (Wall, 2015). An ethnographer researches cultural values, behaviors, beliefs, or languages of social groups of people or organizations (Anderson et al., 2014). Ethnographic researchers immerse themselves in the participants' culture to collect data (Small, Maher, & Kerr, 2014). The ethnographic approach was not suitable for my study because I was not exploring the culture of financial institutions.

Social scientists conducting a phenomenological design study describe and interpret human lived experiences about a phenomenon (Matua, 2015). Phenomenology is the research of lived experiences by humans (Moustakas, 1994). Scholars use

phenomenological design to conduct participant interviews to find common themes (Gill, 2014; Wilson, 2015). The phenomenological design was not suitable for this study because the focus was not on the lived experiences of leaders of a small financial institution.

In this qualitative case study, I collected data through semistructured face-to-face interviews and a review of company documentation. Researchers achieve data saturation when no new themes or codes emerge from the collected data (Higginbottom, Rivers, & Story, 2014). Svensson and Doumas (2013) noted that data saturation occurs when additional data collection efforts result in no new emergent themes. Researchers attain data saturation when a redundancy of information exists (Fusch & Ness, 2015). I collected data through semistructured interviews and a review of company documents, I engaged participants in member checking, and I continued data collection until no new themes or pattern emerged.

Population and Sampling

The targeted population for this study was leaders of a small financial institution. From the targeted population, I used purposeful sampling to identify five research participants from a small financial institution who met the eligibility criteria to take part in the semistructured interviews. Practitioners use purposeful sampling to select participants for a qualitative study who will aid in understanding the research problem and answering the research question. The use of purposeful sampling contributes to the credibility of the findings in qualitative research (Suri, 2011). Palinkas et al. (2015) used purposeful sampling to identify participants with knowledge of the phenomenon under

study. Purposeful sampling in qualitative research is often a solution to practical constraints of time, resources, and access to information (Benoot, Hannes, & Bilsen, 2016). In qualitative data collection, researchers use purposeful sampling to select participants who have the required knowledge and experience to answer the central research question.

Walters (2017) conducted a qualitative case study in financial institutions to explore what strategies financial services leaders use to recruit cybersecurity professionals using a sample size of five financial service leaders. Saber (2016) conducted an exploratory multiple case study of small businesses to investigate cybersecurity strategies and collected data from five small business leaders. Patterson (2017) performed multiple qualitative case studies using 10 small business owners to explore plans that small business owners use to make cybersecurity decisions. Because my research is similar in method and design to the research conducted by Walters (2017), Saber (2016), and Patterson (2017), I considered five participants a proper sample size to perform a single case study in a small financial institution. Eligible research participants for this study were leaders from a small financial institution who implemented strategies to protect information systems from cyber threats. I conducted semistructured face-to-face interviews with participants. The interviews were located in the participants' offices, took 45–60 minutes, and follow-up meetings took 30 minutes. I obtained permission to conduct on-site interviews and gain access to relevant company documents through the CEO or an authorized official of the financial institution signing a letter of cooperation

and confidentiality agreement. I concluded by asking the participants for any company documentation applicable to this study.

Svensson and Doumas (2013) acknowledged that data saturation occurs when no new or related evidence emerges. Orser, Elliott, and Leck (2011) noted that data saturation occurs when continuing data collection only serves to confirm emerging themes. Data saturation transpires when no new themes appear from the added data collection (Ando, Cousins, & Young, 2014). I reached data saturation when no new themes or patterns emerged from my data collection efforts. I used an interview protocol (see Appendix A) to ensure consistency across all the interviews, I engaged the participants in member checking to confirm the accuracy of my interpretation of their responses, I reviewed company documents, and I engaged in methodological triangulation until the no new data emerged.

Ethical Research

Social scientists should recognize that ethical issues might occur when conducting a study involving human subjects. Researchers need to respect the privacy of participants and research partner organizations before, during, and after the data collection process (Sargeant, 2012). Participants should not face the undue risk or have their identities exposed (Yin, 2018). Ethical researchers obtain institutional review board (IRB) approval before recruiting participants and collecting data (Patton, 2002). The purpose of IRB committees was to protect against human rights violations through a thorough review of the potential risks to participants, such as physical injury, emotional stress, or economic harm (Bernard, 2013).

Moustakas (1994) pointed out that qualitative researchers are to follow ethical principles in conducting research involving human subjects and convey the scope of the study, the investigator's role, and expectations of the participants. I obtained the permission of the Walden University IRB before collecting data from participants. After choosing the potential research site and participants, I received the consent of the study site from the prospective financial institutions for inclusion in this study. After receiving approval from the financial institutions and after the IRB granted authorization to start my research, I sent an informed consent form to prospective participants via email. The informed consent form included the following: the purpose of the study, the institution sponsoring the research, any expected risks, and the voluntary nature of the study. The Walden University IRB approval number for this study was 01-29-19-0186113. Ethical researchers obtain informed consent from participants before collecting data (Bernard, 2013). Bhattacharya (2014) noted that research participants should agree to the informed consent form before any interview or questioning to collect data. Cugini (2015) mentioned that informed consent plays a significant function in participants' expectations concerning participation in a study. Participants voluntarily agreed to contribute to this study by replying to the original email of the informed consent form with the words *I consent*.

Participants could withdraw from the study at any time for any reason by any means or no means, and after the start of data analysis, by sending a request via email. Full disclosures of all research practices, policies, and information are actions that lead to

an open atmosphere (Unkovic, Sen, & Quinn, 2016). Participants did not receive payment or any incentives for their involvement in this study.

I used a numbering format RP1 to RP5 as a unique pseudonym to conceal the identity of the research participants. Although the results of this study might include quotes from the participants' responses, the coding format ensured the confidentiality of the small business leaders. Unkovic et al. (2016) noted that participant privacy is an important aspect of ethical research. McDermid, Peters, Jackson, and Daly (2014) said that the use of pseudonyms to hide participants' identities is customary practice in research. Researchers should protect the confidentiality of participants' indemnities by using code names in the published study (Khan, 2014).

I stored the scanned, executed informed consent forms on a password protected flash drive and the original paper copies in my home office. Data from the online questionnaire and semistructured, face-to-face interviews were stored electronically on a password protected flash drive for 5 years after the completion of this study. I securely stored the password protected flash drive and all paper copies of research information in my home office in a fireproof safe. After 5 years, I will electronically delete the files on the flash drive, and mechanically shed paper copies of research records.

Data Collection Instruments

Throughout semistructured interviews, a researcher can act as the data collection instrument through discussions with research participants and in exploring new themes that may arise during the data collection process (Leng, MacDougall, & McKinstry, 2016). The primary data collection instrument in qualitative research is the researcher

(Shields & Rangarjan, 2013). The qualitative researcher roles are to make ease of the interview process, and engage in the sampling, collecting, analyzing, and interpreting the data (Postholm & Skrøvset, 2013). I was the primary data collection instrument for this study. I used semistructured interviews and organizational documents as data collection instruments.

I used semistructured interviews to elicit information-rich data from the research participants via face-to-face discussion (see Appendix A). Scholars widely use semistructured interviews in qualitative research (Cridland, Jones, Caputi, & Magee, 2014). Participants are free to respond to the interview questions, while the researcher can ask probing questions to the responses (Shan et al., 2015). Jamshed (2014) noted that semistructured interviews consist of participants answering preset, open-ended questions. Scholars use an interview protocol as a guide to conduct semistructured interviews (Jamshed, 2014; Merriam & Tisdell, 2015). I used an interview protocol as a guide to conduct the interviews (see Appendix A). Yin (2018) noted that researchers ask the same interview questions to different research participants to obtain a diverse range of answers and interactions. I used semistructured interviews to explore the strategies some leaders of a small financial institution use to their protect information systems from cyber threats.

The format for the semistructured interviews included open-ended and probing questions. Practitioners used open-ended questions as a proper data collection instrument to gather perspectives and information from participants (Bernard, 2013). Bryman (2012) suggested that open-ended interview questions are the best data collection tool for researchers to address the qualitative research problem and answer the central research

question. I used open-ended interview questions to provide the participants with an opportunity to give a complete description, as well as expound on and expand the discussion of the strategies used to protect information systems. I used organizational documentation as a data collection instrument. Scholars often time use literature as a data collection instrument (Linton, 2017; Weldearegay, 2017).

Participant observations during the semistructured interviews provided researchers with ways to check for nonverbal expression of feelings, decide who interacts with whom, grasp how participants communicate with each other and check for how much time spent on various activities (Denzin, 2012; Marshall & Rossman, 2016). Yin (2018) responded that researchers collected data from interviews, documentation, archival records, direct and participant observation, and physical artifacts that are sources of data for performing a case study. I used participant observations as a means of watching the behavior of participants during the semistructured interviews.

Peters and Halcomb (2015) pointed out that interview protocols included the script for pre and post-interview protocols, interviewer prompts to collect informed consent, and interviewee reminders of the research purpose. Boddy (2016) asserted that interview protocols are a set of questions and procedural guide for directing a new qualitative researcher through the interview process. Leins, Fisher, Pludwinski, Rivard, and Robertson (2014) recognized that a proper interview protocol is essential for accurate information retrieval from study participants. I strived to ensure the participants remained focused on directly answering the interview questions (see Appendix A).

I used member checking and methodological triangulation as a means of quality control in the data collection process. I used member checking to ensure the accuracy of data and my analysis of the research participants' responses. Morse (2015) commented that researchers use member checking to improve the dependability and credibility of the findings of a qualitative study. Social scientist acknowledged member checking as the last step in a qualitative research validation (Fusch & Ness, 2015). Member checking ended the possibility of misconstruing the data and taking the interviewees' responses out of context (Stack, Sahni, Mallen, & Raza, 2013). I strived to minimize errors in the interpretation of participant meaning by using member checking. After the semistructured interviews, I transcribed the audio recordings of the participants' responses. Every participant in this study received a one-page summary of my interpretations of the transcribed interview for member checking via email or in person. I allowed the participants to discuss my analysis of their discussions in a 30-minute member checking session within five days of the first meeting. I also asked to follow up questions after my observation to clarify interview interpretations in addition to having the opportunity to ask added questions until I achieved data saturation.

Methodological triangulation is a method used in qualitative research to improve the credibility and dependability of the study and evaluation of findings (Rubin & Rubin, 2012). Methodological triangulation is a method of collecting data from multiple sources (Denzin, 2012; Yin, 2018). Renz, Carrington, and Badger (2018) used methodological triangulation to strengthen the design of qualitative research to increase the ability to interpret findings from multiple data sources. Practitioners use triangulation as a strategy

for qualitative research to test the dependability and credibility of the data through the merging of information from some sources (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). I used participants' responses and company documentation to build a logical explanation of the themes by exploring evidence from the sources.

Data Collection Technique

Researchers conducting a qualitative case study collect data through multiple methods, such as interviews, archived records, and observation (Ravitch & Carl, 2016). I obtained data from five business leaders from one small financial institution in Doha, Qatar using face-to-face, semistructured interviews with probing questions, notes from interview observations, and analysis of company documentation, such as public or confidential information about cybersecurity strategies, cybersecurity policies, and employee handbooks. Scholars conducting a qualitative case study collect their data by using multiple techniques to engage in methodological triangulation (Fusch & Ness, 2015; Namukasa, 2013; Ravitch & Carl, 2016).

I used an interview protocol as a guide for collecting the interview data (see Appendix A). The interview protocol has language about the open-ended questions, a script for what I planned to say before and after the interviews, and the process of obtaining informed consent from the participants. Lewis (2015) noted that researchers use an interview protocol as a guide to maintain a consistent interview process. The interview protocol process included opening with a review of the study's purpose, explaining the informed consent process, overviewing the interview format, clarifying the time allotted, and inviting participant questions (Bernard, 2013). Using the interview protocol allowed

me to obtain detailed and rich descriptions of the participants' knowledge and ability to implementing cybersecurity strategies. I used semistructured interviews as a data collection technique to ask open-ended questions. An interview is a discussion with someone in which the researcher attempts to obtain information from the interviewee about the phenomena (Thomas, 2013). The semistructured interview is useful when a deep understanding of participants' experience of an event is necessary (Pistol & Rocsana, 2014).

Researchers should align the interview questions with the overarching researching question of the study (Qu & Dumay, 2011). I used semistructured interviews to elicit answers focused on the strategies used by leaders to protect information systems from cyber threats (see Appendix A). Each participant responded to the same interview questions. Yin (2018) noted that investigators seek participants' responses to the same interview questions to compare the collected data. Semistructured interviews were an effective means of collecting information-rich data from participants.

I found a financial institution through publicly available online business directories: the Qatar Online Directory (http://www.qataronlinedirectory.com/), Qatcom.com (http://www.qatcom.com/), and ezyQatar (http://www.ezyqatar.com/). I obtained Walden University IRB approval before contacting leaders of financial institutions. I contacted the CEO of the financial institution to get permission to contact leaders within the institution via email or telephone. I obtained a signed Letter of Cooperation and Confidentiality agreement from the CEO. I asked for potential business leaders' contact information within the institution to take part in the study. I emailed an

invitation with an informed consent attached. The participants supplied informed consent by replying *I consent*. After receiving the informed consent, I coordinated a time with the participants to schedule the face-to-face interview. All interviews lasted 45-60 minutes with a 30-minute follow-up meeting. I followed the same interview protocol of a brief introduction followed by the presentation of the interview questions. I recorded interviews using the iPad/iPhone recorder app as well as taking detailed notes as a backup. I then transcribed the recorded interviewee responses in Microsoft Word and then shared with the participants for review. Once I reviewed the transcribed interview corrected by the participants, the documents will be upload into QSR NVivo 12 to find codes and themes. I will save the transcribed documents in Microsoft Word and NVivo on my password-protected computer for 5 years.

The advantage of using face-to-face semistructured interview recorded with an audio digital documented and analysis of company documentation is giving a correct screening of participants' nonverbal cues (Alby & Fatigante, 2014; Erlingsson & Brysiewicz, 2013; Pistol & Rocsana, 2014; Yin, 2018). Using face-to-face, semistructured interviews is a means for researchers to create an environment for the participants to have the freedom to share in an open exchange to garner rich, in-depth responses to aid in answering research questions (Alby & Fatigante, 2014; Erlingsson & Brysiewicz, 2013; Pistol & Rocsana, 2014; Yin, 2018). The disadvantage of using face-to-face semistructured interview is the indirect information filtered through the views of interviewees. A researcher's presence may cause bias responses, and not all participants are equally articulate and perceptive (Bernard, 2013; Yin, 2018). Marshall and Rossman

(2016) explained the disadvantages of interviews conducted face-to-face are time consumption of recruiting participants and conducting interviews, cost of conducting interviews because of timing and traveling, interviewees can deliver biased responses, and most carefully vet the respondent's ability before investing time in the recruitment process and interview process.

The next data collection technique I used is the financial institution's public or private documentation. Public documentation may include meetings from meetings or official reports (Thomas, 2013). Private documentation may consist of journals, diaries, or emails (Thomas, 2013). Obtaining contextual language and words of participants in documentation is an advantage of documentation (Lewis, 2015). Researchers can access the documentation at a time convenient to the researcher, which is an unobtrusive source of information (Lewis, 2015). Documentation is data that are thoughtful in that participants have given attention to compiling them, and as written evidence, documentation saves a researcher the time and expense of transcribing (Lewis, 2015). Investigators posited that the disadvantages of literature are the protect information unavailable to public or restricted access, needs the researcher to search out the information in hard to find places, needs transcribing or optically scanning for computer entry, and material may be incomplete, and the documents may not be authentic or correct (Lewis, 2015; Thomas, 2013).

I used member checking to ensure the accurateness and legitimacy of data within participant responses relating to the outcomes and theme of this study. Every interviewee received a summary of my interpretation of the transcribed interview via email for

member checking to ensure credibility. Researchers use member checking to assure the credibility of research (Lub, 2015). Morse (2015) explained that in member checking, the researcher functions on the supposition that the degree to which members acknowledge their experiences in research products determines the dependability of research claims. Scholars use member checking to give research participants a chance to evaluate a researcher's interpretation, to correct misinterpretations, and offer more information that appeared from the interview process (Fusch & Ness, 2015). I used member checking to allow the research participants the opportunity to confirm their interview responses, as well as improve the credibility, dependability, and accuracy of the findings of this study.

Researchers conduct a small pilot study to evaluate the procedures, instruments, and methods for a more extensive study to follow (Wray, Archibong, & Walton, 2017). The purpose of conducting a pilot study is to verify that the chosen research method, design, and data collection instruments are appropriate to conduct a large-scale study (Patton, 2002). Wray et al. (2017) noted that researchers use a pilot study to know whether the interview questions are understandable and align with the central research questions. A researcher conducts a pilot study in advance to test the aspects of the research design and make a necessary adjustment before the research (Doody & Doody, 2015). I was conducting a limited scope case study and did not need to conduct a preliminary small-scale study to prepare for a larger research project.

Data Organization Technique

I organized the collected data by using pseudonym codes to match participants with their responses. I then arranged the received data in a digital folder on an external

hard drive by participants and interview date. Bernard (2013) explained the process of organizing the collected data involved data checking, keeping, and reviewing a reflective journal throughout the study, entering raw data into qualitative data analysis software, and reviewing researcher notes. Pinfield, Cox, and Smith (2014) explained that data organization techniques entail the structure, storage, safety, and retrieval of data. Korhonen (2014) explained that the efficient organization of data enabled the proper storage of data and analysis for effective communication of the study's findings.

I used Microsoft Word software to type the transcription of each interview recording. I provided each participant with a password-protected file that has a copy of the interview transcript. Investigators should create a dedicated file for each participant (Welch, Grossaint, Reid, & Walker, 2014). Upon participant approval, the transcription extraction occurred from Microsoft Word for the next import into QSR NVivo software. I organized and analyzed participants' responses using QSR NVivo. Chittem (2014) noted that computer-assisted, qualitative analysis software, such as QSR NVivo, are useful tools for researchers to organize and analyze. Edwards-Jones (2014) explained that QSR NVivo is a qualitative, data analysis tool used for coding, collating, and analyzing data. For this qualitative case study, an import of all participant data took place in QSR NVivo for thematic coding.

Using codes represented the identities of the participants served to ensure confidentiality. A social scientist employed the use of codes to provide the participants' privacy (Patton, 2002; Yin, 2018). Bradley, Getrich, and Hannigan (2015) noted that using QSR NVivo® software program enabled the development of a codebook to

organize data, build narrative summaries, and conduct a cross-case analysis of interview data to address the research questions. The code for each research participant consisted of the letters RP, meaning Research Participant, followed by numbers from 1-5 to ensure the confidentiality of the participants and the organization's identity. I organized data by the research participant number to access the raw data quickly. Therefore, I coded participants as RP1, RP2, RP3, RP4, and RP5.

Keeping self-reflective study journals is an approach that can aid in reflexivity (Newington & Metcalfe, 2014). Using reflective journals enabled qualitative researchers to organize and develop their experiences, opinions, thoughts, and viewpoints visible and acknowledged as part of the research (Newington & Metcalfe, 2014). Applebaum (2014) affirmed that keeping a self-reflective research journal is a strategy that eases reflexivity; researchers use their journal to find personal assumptions and goals and clarify individual belief systems and subjectivities. To minimize researcher bias, I kept a journal to document personal reflections and observations that might show any personal partiality during the data collection process or add to the study. I did not select participants with whom business or personal relationship exists. The means for organizing and storing the participants' transcribed responses will involve using a password protected external hard drive stored in a locked safe for 5 years. After 5 years, data is destroyed by removing electronic files and shredding of paper files.

Data Analysis

The process of data analysis involved making sense out of the text data. The data analysis process consisted in preparing the data for analysis, conducting difference

analysis, moving deeper and deeper into understanding the data, being the data, and making an interpretation of the broader meaning of the data (Yin, 2018). Scholars gain an understanding of a phenomenon in qualitative research by uncovering hidden patterns, concepts, and themes in the data analysis process (Bedwell, McGowan, & Lavender, 2015; Gioia, Corley, & Hamilton, 2012). I used the conceptual framework of actor-network theory as the lens during data analysis. To analyze data, I used Yin's (2018) five-step data analysis process of compiling the data, disassembling the data, reassembling the data, interpreting the meaning of the data, and concluding the data.

Scholars used methodological triangulation during data analysis to improve the credibility and dependability of research of findings (Rubin & Rubin, 2012). Renz et al. (2018) noted that methodological triangulation is a means for the researcher to strengthen the analysis of qualitative data through crosschecking data collected from multiple sources. Researchers used methodological triangulation to test the dependability and credibility of the data through the convergence of information from various sources (Carter et al., 2014). I collected data through multiple methods, crosscheck interview data with documentation data, and built a coherent justification for themes using methodological triangulation.

Compiling Data

The first analytical phase of collecting data into a formal database is the careful and methodic organizing of the original data (Yin, 2018). I received the data from the transcribed interviews and documentation using QSR NVivo qualitative software. I proofread the text and listen to audio records to gain a deeper understanding of the data.

Moustakas (1994) defined epoché as the process of setting aside prejudgments in research to remove bias. The purpose of epoché was for researchers to set aside prejudices and preferences to ensure that the study is pure (Bazzano, 2014). Patton (2002) stated that epoché was the process by which a researcher takes on a phenomenological approach to end personal bias. I set aside my prejudices and worldview during data analysis to mitigate bias.

Disassembling Data

The second phase of the analysis included breaking down the compiled data into smaller fragments or pieces (Essary, 2014; Yin, 2018). Cox and McLeod (2014) stated that when disassembling data, themes appeared from the data and emerged, keywords and commonalities appeared, which allowed for coding. Researchers disassemble data by dividing the data into labels and fragments (Yin, 2018). Yin (2018) noted that the disassembling procedure could be repeated many times as part of a trial and error process of testing codes, accounting for the two-way arrow between these the compiling and disassembling phases (Yin, 2018). I used QSR NVivo in the data disassembling process. I coded and categorized data based on keywords and ideas shown in the themes from the literature review.

Reassembling Data

Reassembling data is the phase in which case study researchers use substantive themes to reorganize the disassembled fragment or pieces into different groupings and sequences that might have been in the original notes (Yin, 2018). The third phase is reassembling data (Yin, 2018). The reassembling process involved in clustering and

categorizing the labels into a sequence of groups (Yin, 2018). Scholars ease the rearrangements and combinations of data by depicting the data graphically or by arraying them in lists and other tabular forms. Reviewing the information repeatedly helps to find the emergence of the same and or different patterns in the data (Baškarada, 2014; Yazan, 2015). I used the search, query, and visualization tools in QSR NVivo to find connections and patterns in and between the categories, and sort and reassemble the data into themes. As new themes appeared, I created a new group and scanned all the data again to decide if I should code added data with the original idea. Niedbalski and Ślęzak (2016) explained that QSR NVivo® software reinforced qualitative data analysis through managing and organizing data, managing ideas, querying data, and reporting results from the data. Garfield, Hibberd, and Barber (2013) explained that themes appeared through the QSR NVivo®.

Interpreting Data

The fourth phase of Yin's (2018) five-step of analysis involves the reassembled material to create a new narrative, with accompanying tables and graphics relevant that will become the critical analytics part of the study. The interpretation stage occurred when the researcher develops narratives and conclusions from the reassembled data (Yin, 2018). The interpretation stage involves creating stories from the sequences and groups for findings (Fusch & Ness, 2015). During the interpretation stage, Essary (2014) suggested that researchers find a deeper meaning from the data. Yin pointed out that a researcher should have developed some data arrays or other ways of reassembling the data. Investigators should have in mind how an empirically based interpretation of the

data has appeared (Yin, 2018). Initial analysis of data leads to the desire to recompile the database in a new way, or to assemble the data differently, all the sequences in the study represented by the separate one way and two-way arrows (Yin, 2018). As suggested by Marshall and Rossman (2016), the member checking process is a review of a summary of the data interpretations by participants. I engaged the participants in member checking, which ensured a correct analysis of the interview data.

Concluding Data

In the last step, I critically thought about the data and reflected on what I had learned about the strategies used in the cybersecurity development process. Yin (2018) noted that researchers should give some thought to the conclusions made by the research. Compelling findings bring unity to the entire rest of the study (Yin, 2018). Yin mentioned findings relate to the interpretation in the interpreting phases and through all the other steps of the five-step data analysis process. The conclusions would encompass the meaning of the data (Yazan, 2015). Cox and McLeod (2014) noted that findings from the data analysis included the report of findings and tables to explain results. I assessed what the categories and patterns mean, and significant of the central research question. I continued to use newly published studies to help substantiate emerging themes and relate the results to the conceptual framework and the general body of literature.

Software Plan

Computer-aided qualitative data analysis is a significant part of research projects (Davidson, Paulus, & Jackson, 2016). The purpose for researchers to use QSR NVivo software program was to help coding, organizing, and placing the data into themes

(Edwards-Jones, 2014). Researchers used QSR NVivo software to assist in analyzing interview transcripts and helping data management (Bradley et al., 2015; Castleberry, 2014; Cridland et al., 2014). I used the auto-coding feature within QSR NVivo to find and link similarities in data with propositions and emerging themes as well as reviewing the data manually for redundancy, checking for accuracy, and finding topics within the data. I used Microsoft Word to enter the responses of each recorded interview. I made available for each participant a password-protected file, possessing a copy of the interview transcription, for participant review and written endorsement.

Key Themes

The key themes from the data will correlate to the actor-network theory and strategies used by business leaders for cybersecurity strategy. Scholars used the actor-network theory to aid in the understanding of how systems make both structural and functional changes (Young et al., 2012). Bossong and Wagner (2017) supplied a nuanced, more focused, yet nonetheless critical reading of public-private partnership for cybersecurity. Bossong and Wagner posited that the first heuristic typology showed companies are one part of the more extensive governance processes in this field. I examined the data through the lens of the actor-network theory to build on themes about potential strategies used by business leaders to protect information systems from cyber threats for the safety of individuals. Identification of the emergent themes will help answer the overarching research questions and may give exploratory information on the common factor that can affect cybersecurity strategies by business leaders. I used the results from the participant interviews to address the research questions.

Reliability and Validity

Scholars conducting qualitative studies seek dependability of the data and the research findings instead of reliability (Hill & Bundy, 2014). Researchers showed that when designing, analyzing, and judging the quality of a study; qualitative researchers should address credibility and dependability (Morse, 2015). Qualitative researchers seek credible, confirmability, trustworthy findings (Titze, Schenck, Logoz, & Lehmkuhl, 2014).

Dependability

Dependability is the constancy of the research data (Rydwik, Bergland, Forsén, & Frändin, 2012). Marshall and Rossman (2016) showed that researchers used member checking to verify the accuracy and completeness of the interview findings, contributing to the dependability of a study. A researcher strives for reliable data and findings by using a strict interview protocol and engaging the participants in member checking to verify the accuracy of the interview data (Frels & Onwuegbuzie, 2013; Marshall & Rossman, 2016; Thomas & Magilvy, 2011). I adhered to a strict interview protocol and engaged the participants in member checking to ensure dependable data and findings.

Moustakas (1994) noted in qualitative research studies, the systematic compilation of data could address dependability. Patel, Shah, and Shallcross (2015) showed that interview protocols are instructions interviewers follow to ensure consistency between interviews, which increased the dependability of the study findings. De Ceunynck, Kusumastuti, Hannes, Janssens, and Wets (2013) acknowledged that the interview protocol is guided for the researcher to complete the interview procedure and

includes the interview type, format, and goal. I followed the interview protocol (see Appendix A) to ensure the participants still are focused on answering the interview questions, which are in alignment with the research question.

Credibility

Credibility is the genuineness of the research data from the participants' views (Cope, 2014). Scholars use member checking to enable participant validation of the completeness and correct understanding of participants' responses as captured by the researcher (Marshall & Rossman, 2016; Thomas & Magilvy, 2011). Researchers use the two sources for data collection to allow the use of methodological triangulation to support the findings from the data as well as to improve the credibility and confirmability of the study (Houghton, Casey, Shaw, & Murphy, 2013; Yin, 2018). I used member checking and methodological triangulation to ensure credibility.

Confirmability

Researchers strive for confirmability by ensuring the data emanated from the participants' responses, not the researcher's opinions, preconceptions, or worldview (Cope, 2014). Confirmability is the degree to which other researchers confirm or corroborate the findings of a study (Treharne & Riggs, 2015). Houghton et al. (2013) suggested that researchers must ensure a level of confirmability to assure research rigor. Anney (2014) mentioned using a self-reflective journal toward setting up confirmability. Investigators use methodological triangulation to strengthen the confirmability of their case study (Yin, 2018). A social scientist should use data saturation to enhance conformability (Teusner, 2015). Confirmability addresses the manner to which

researchers receive a confirmation of the findings or results (Hanson, Balmer, & Giardino, 2011). I asked probing questions during interviews, engaged participants in member checking, used methodological triangulation, and reached data saturation to ensure the confirmability of the findings of this study.

Transferability

Cope (2014) defined transferability as the applicability of the study findings to other cases, groups, or settings, as noted by the reader of the study or future researchers. Scholars denoted transferability as the transparency of the researcher with moving the collected research data in a full description that enabled the reader to understand the framework of the study (Alex da, Näslund, & Jasmand, 2012). Researchers' contextual stories helped the transferability of research findings to other settings with similar context (Erlingsson & Brysiewicz, 2013). Erlingsson and Brysiewicz (2013) suggested that researchers should encourage the participant to respond to the interview with thick, rich description to ensure transferability in a similar context by using procedures to supply correct information for credibility. According to Yin (2018), information about the researcher, population studied, sampling, and coding decisions supplies to improve the prospect of transferability, but a case study researcher cannot assure transferability. To enhance the opportunity for future researchers to transfer the findings of this study to other cases and settings, I provided rich descriptions of my research process and results in Sections 3. I reached data saturation, engaged in methodological triangulation, and ensured the credibility of the findings to help improve the prospects for transferability of the results by future researchers.

Data Saturation

I collected data through semistructured interviews and a review of company documents, engage participants in member checking, and continue data collection until no new themes or pattern appear. Higginbottom et al. (2014) stated that data saturation is when no new themes emerged from the collected data. In agreement with Higginbottom et al. (2014), Svensson and Doumas (2013) pointed out that when no new information emerged from data collection, this is data saturation. Fusch and Ness (2015) advanced that the amount of repeated information or data that gave no added perceptiveness during the data collection signaled data saturation.

Transition and Summary

The purpose of this qualitative single case study was to explore small financial institution leaders' strategies to protect information systems from cyber threats. The role of the researcher was to act as the primary data collection instrument in qualitative research. My role as the researcher was to adhere to the research standards outlined in the Belmont Report, mitigate biases, and ensure dependable, credible findings. The eligibility criteria for participants in this study were leaders of a small financial institution in Doha, Qatar, who implemented a successful strategy to protect information systems from cyber threats. Semistructured interviews and company documentation was the sources of data. Yin's (2018) five-step process of compiling, disassembling, reassembling, interpreting, and concluding the data is the selected means for analyzing the data. The use of methodological triangulation, using member checking, and reaching data saturation were the means to ensure dependable, credible, confirmable, trustworthy findings.

Section 3 contains the presentation of the findings along with how the findings of this study confirm or refute the findings of previous researchers who conducted studies on a similar topic. Section 3 contains an explanation of the applications to professional practice, implications for social change, and recommendations for further research. The section concludes with my reflections and a closing statement.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative study was to explore the strategies that leaders of a small financial institution use to protect information systems from cyber threats. I collected the data in this study from leaders of a small financial institution using semistructured interviews and a review of company documents. Four themes emerged from the results of the data analysis: (a) information security management, (b) cybersecurity policy, (c) risk management, and (d) organizational strategy. This section of the study contains a presentation of the findings, applications to professional practice, implications for social change, recommendations for action, recommendations for future research, reflections, and a conclusion.

Presentation of the Findings

In the presentation of the findings, I addressed the overarching research question: What strategies do leaders of a small financial institution use to protect information systems from cyber threats? The targeted population for this study was leaders of a small financial institution in Qatar. From the targeted population, I used purposeful sampling to identify five research participants from a small financial institution who met the eligibility criteria to take part. I collected data through semistructured interviews and a review of company documents, I engaged participants in member checking, and I continued data collection until no new themes or pattern emerged. I used the conceptual framework of actor-network theory as the lens for this study. To analyze data, I used Yin's (2018) five-step data analysis process of (a) compiling the data, (b) disassembling

the data, (c) reassembling the data, (d) interpreting the meaning of the data, and (e) concluding the data. I prepared the data for analysis by conducting difference analysis, moving deeper into understanding the data, and making an interpretation of the broader meaning of the data.

Each participant's involvement in this study was voluntary. All research participants replied with *I consent* to an emailed informed consent form. The research participants agreed to contribute to the study through audiotaped, 45–60-minute face-to-face interviews and 30-minute follow-up meetings for member checking. I obtained access to a variety of company documents through the authorized official of the company by signing a research partner letter of cooperation. I used methodological triangulation and member checking to reach data saturation to ensure dependable, credible, confirmable, and trustworthy findings. I used Microsoft Word to enter the transcribed responses of each recorded interview. I then uploaded the Microsoft Word documents into QSR NVivo Plus 12 to organize and analyze the data into themes, as recommended by Edwards-Jones (2014). Theme development aligned with the conceptual framework and literature review provided in Section 1 of this study.

The conceptual framework for this study was Law's (1992) actor-network theory. Wairokpam and Kumar (2018) stated that actor-network theory is a toolkit for leaders to explore how human and nonhuman actors interact with one another to make sense of their world. Iyamu and Mgudlwa (2018) pointed out that actor-network theorists aim to explore the process of building or assemblage and maintenance of networks to achieve an objective. Lukka and Vinnari (2017) characterized actor-network theory as an approach

that researchers use to focus on the relationships forged between human and nonhuman objects in material-semiotic networks.

Previous research on the cybersecurity strategies that leaders of small businesses have used to protect their systems from cyber threats was deficient in academic standards, as I discussed in the literature review in Section 1 of this study. Because of the limited information available about strategies that small financial institutional leaders have used to protect their systems from cyberattacks, research opportunities were available. The analyzed data I collected from semistructured interviews, member checking, and a review of company documents led me to answer the overarching research question: What strategies do leaders of a small financial institution use to protect information systems from cyber threats?

Four themes pertinent to the research emerged from my data analysis: (a) information security management, (b) cybersecurity policy, (c) risk management, and (d) organizational strategy. For confidentiality purposes, I referred to the participants in this study as RP1, RP2, RP3, RP4, and RP5, and referred to the financial institution as the Company. Table 1 is a display of the top 10-word frequency query results, which I used during data analysis in conjunction with the full interview transcripts and document data to develop the four themes for this study.

Table 1

Word Frequency Query Results

Word frequency query	Number of occurrences
Security	126
Information	62
Systems	43
Policies	41
Network	37
Risk	34
Management	31
Cyber	29
Access	26
Threats	26

In Table 2, I display the four key strategies the leaders of the financial institution used to protect their information systems from cyber threats.

Table 2

Emergent Themes

Theme	# of participants who contributed to the theme	Participant ID
Information security management	4 of 5	RP1, RP2, RP4, RP5
Cybersecurity policy	5 of 5	RP1, RP2, RP3, RP4, RP5
Risk management	5 of 5	RP1, RP2, RP3, RP4, RP5
Organizational strategy	4 of 5	RP1, RP2, RP3, RP5

Figure 1 is a mind map to display the interlinking aspects of the strategies and tactics the leaders used to protect their information systems from cyber threats.

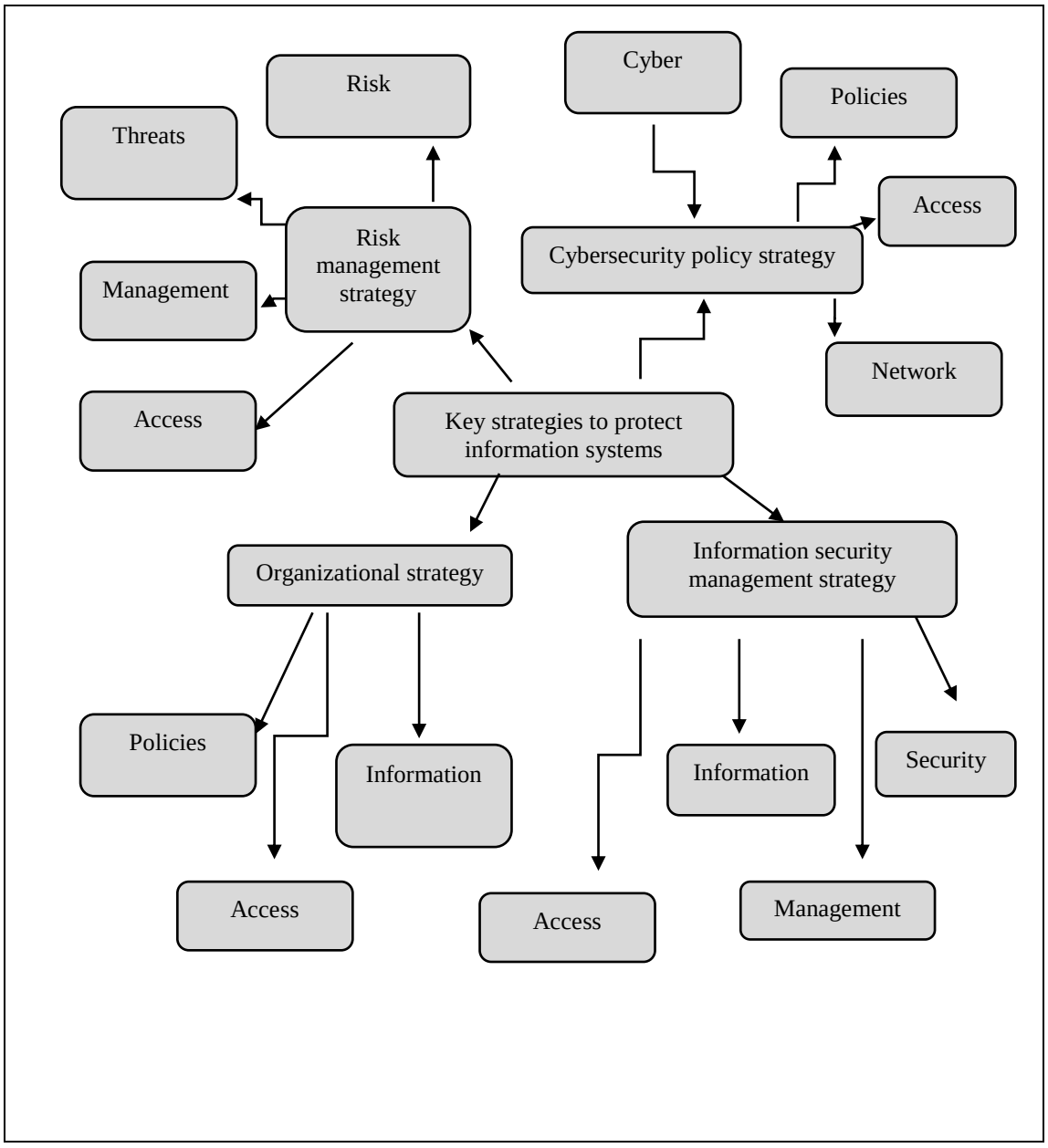

Figure 1. Mind map for key theme strategies and subthemes.

I reviewed a variety of company documents to engage in methodological triangulation to crosscheck and validate the interview data. In Table 3, I displayed the

documents reviewed to corroborate the key themes for strategies used by the leaders of the Company.

Table 3

Documents Reviewed to Corroborate Key Theme Strategies

Documents	Information security management	Cybersecurity policy	Risk management	Organizational
Back up policy	x	x	x	
Firewall policy	x	x		
Network security policy	x	x	x	x
Password policy	x	x		x
Patch management policy	x	x	x	
Virtual private network standards	x	x	x	
Wireless security policy	x	x	x	
Critical risk indicator report	x	x	x	x
Antimalware and spam policy	x	x	x	
Access control policy	x	x	x	x
Acceptance usage document	x	x	x	x

Theme 1: Information Security Management Strategy

The first major theme in this study was an information security management strategy. The information security management strategy theme emerged from the responses of four participants and from company documents. The four research participants stressed the importance of an institutional information security management policy and process. Information security is the practice of preventing unauthorized

access, use, disclosure, disruption, modification, inspection, recording, or destruction of information (Wang, Zhe, Gupta, & Rao, 2019). The information or data may take various forms, such as electronic or physical information, for leaders to focus on the equal protection of the confidentiality, integrity, and availability of data while maintaining a focus on efficient policy implementation, all without hampering organization productivity (Paliszkiewicz, 2019).

Feng and Wang (2019) noted that financial institution leaders must go through a multistep risk management process to identify assets, threat sources, vulnerabilities, potential effects, and controls, followed by an assessment of the effectiveness of the risk management plan to ensure information security. RP5 stated, "We are integrating our strategy of protecting our information systems from cyber threats by publishing well-defined information security policies and security standards to all staff and departments in our bank under the sponsorship of the risk department." In agreement with RP5, RP1 mentioned, "Establishing a successful information security program begins with strong upper-level management support. This support establishes a focus on security within the highest levels of the organization." RP4 acknowledged, "We have clear information security policies and procedures for every department and employees." RP2 stated,

> We implement a business continuity plan to regularly make backup copies of the bank's data and information. To encourage affiliation with the most efficient companies to respond against any cyberattack or the breach, and to conduct regular information security testing on infrastructure security and external penetration testing to ensure compliance to the bank's applied protection

procedures and tools, and to the applied security framework against any possible cyber threat.

The goal of information security management is to minimize risk and ensure business continuity by proactively limiting the effect of a security breach (Tu, Yuan, Archer, & Connelly, 2018). RP5 stated, "Management shows significant interest and importance to make all the organization's staff informed and educated about security threats and preventive security standards and policies addressing cyberattacks." I reviewed the acceptance usage, access control, antimalware and spam, backup, firewall, critical risk indicator report and areas of assessment, network security, password policy and standards, virtual private network security standard, and wireless security policy documents to triangulate the data. I reviewed the Company's backup policy that the leaders discussed during the interviews as a means to ensure business continuity. I included some excerpts from the company documentation as examples of triangulating and crosschecking the interview with the data collected from the documentation. The Company's backup policy document contained the following:

> Backups are a business requirement to enable the recovery of data and applications in case of events such as natural disasters, system drive failures, espionage, data entry errors, or intentional destruction.
>
> This policy covers all data and application that are essential to the continued operations of the organization. The policy applies to all application owners, system administrators, network administrators, security administrators, and operators who are responsible for the backup, restoration and security of all

> data and application that are essential to the continued operations of the organization.

I used the backup policy to corroborate RP1, RP2, and RP5's interview response regarding security policies addressing data protection, the confidentiality of information, and the best-secured practices using the bank's information assets and systems. RP1 noted,

> We have to ensure the development and implementation of the institution information security policies, standards, and procedures and ensure timely updating thereof in light of changing circumstances, best practices, and regulatory directives. The focus and objective are to develop those standards and policies based on the institution's needs and requirements; in other words, in-house built and cultivated internally to guide the institution workforce.

RP4 pointed out that their organization has clear information security policies and procedures for every department and employee. RP1 stated,

> Developing an information security strategy in support of business strategy and direction and create the program in full view while working with the other components of the organization the program must meet the needs of the organization and not just be an implementation of advanced controls.

The information security management theme that emerged from the data confirmed and aligned with the findings of Ducas and Wilner (2017), Choi, Martins, and Bernik (2018), and Singh and Gupta (2019) in that information security management is a practice needed to protect information systems from cyber threats. Ducas and Wilner

(2017) acknowledged that information security had become a central issue of information technology management and academic researchers. The technological and societal developments, because of the rapid changes in technology and society from information security, impelled many organizations to the development of information security management (Choi et al., 2018). Singh and Gupta (2019) suggested the framework for information security management along with their key identified factors were external, such as changing security threats, risks, the legal and regulatory environment, standards, and market situations, whereas business issues, project outsourcing, information technology infrastructure, organizational policies, and objectives constitute the internal factors. All participants in this study suggested well-defined information security policies and standards for all employees are strategies for protecting information systems from cyber threats.

Theme 2: Cybersecurity Policy Strategy

A cybersecurity policy strategy was the second major emergent theme in this study. The cybersecurity policy strategy theme emerged from the responses of all research participants and the supporting documents. Cybersecurity is a process of leaders using tools, policies, security models, security precautions, strategies, risk management tactics, activities, preparation, best practices, and technologies to protect the cyber atmosphere, institutes, and user data (Reid & Van Niekerk, 2014). Small businesses are at the same risk for cyberattacks as larger companies (Mansfield-Devine, 2016). All participants noted the importance of the Company implementing and using a cybersecurity policy. RP1 and RP2 commented on the critical aspects of the

cybersecurity policies and the need for guidelines to support a robust cybersecurity strategy to ensure regulatory compliance, information systems' protection, and protection of customer data. Business leaders use technology, management procedures, organizational structure, laws, regulations, and human competence to implement effective cybersecurity policies (Elkhannoubi & Belasissaoui, 2016). RP1 stated, "Focusing on the need for a stable security governance program to be in place so all security strategies and processes can be planned, designed, implemented, and maintained is vital to our survival." I crosschecked the interview data with the password policy and standards document, which contain the following excerpt: "It is the responsibility of the information technology security manager to keep this policy and standard current and adequate and ensure full compliance against all security standards implemented in the bank."

Li et al. (2019) acknowledged that leaders use a cybersecurity policy to communicate the best practices for users to limit the potential for attacks and ameliorate the damage. RP4 stated, "We are always communicating the latest updates concerning the cybersecurity threats with our staff. We applied an easy way of communicating any suspicious cybersecurity threat, and we encouraged the feedback with the information technology department." RP5 acknowledged, "One of the practical aspects of the cybersecurity strategy is to communicate the security awareness updates to all our staff in all the departments on a regular basis." RP3 noted that communication of the cybersecurity policies to employees occurred by the Company's policy and procedural documents, internal memos, periodic information security training, and circulated

information via email. This finding confirms the research of Park, Kim, Kim, and Lee (2018), who stated that communicating cybersecurity policies to the employees is an essential duty of organizational leaders to protect information systems and maintain a culture of information security.

Elkhannoubi and Belasissaoui (2016) pointed out that a security policy establishment starts with the direct participation of regional and local authorities, public and private sector leaders, and government officials working in tandem with company leaders. RP2 expressed, "From my point of view, I would be recommending to the bank or any reputable financial institution ways to update its information about the cybersecurity events and the most updated ways and tools to protect themselves from cyberattacks." An excerpt from the Company's cybersecurity policy contain the following excerpt: "The objective of this policy is to protect the Company, customer information, and data from unauthorized modification, damage, or deletion resulting from accidental or intentional attempts to gain access to or compromise the Company systems."

All participants discussed the importance of developing a cybersecurity strategy that best fits the needs of the organization. Cybersecurity policy is a set of policies issued by an organization to ensure that all information technology users in the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority (Hewett, Kijsanayothin, Bak, & Galbrei, 2016). RP3 stated, "A set strategy integrated with the bank's policy and procedures to respect all related rules

and regulations is one way we use our cybersecurity policy." The finding of a cybersecurity policy strategy aligns with the research of Bodin, Gordon, Loeb, and Wang (2018) who noted that effective business leaders employ information security policies to protect their digital assets and intellectual rights in efforts to prevent theft of industrial secrets and information that could benefit competitors. Schneider (2018) noted that as cyberattacks become the new standard, having a cybersecurity policy became not just a matter of information security, but of saving money, data, and valuable employee resources. All participants recommended having a clear information security policy and procedure for every department as a strategy for protecting information systems from cyber threats. Research participants' responses and company policy documents indicated that cybersecurity strategies were of the highest importance to the Company's leaders.

The leaders of the small financial institution I collected data from recognized the need for effective cybersecurity policies to implement their strategy to protect information systems. The Company had in place a variety of policies regarding information and cybersecurity. I reviewed the acceptance usage, access control, antimalware and spam, backup, firewall, critical risk indicator report and areas of assessment, network security, password policy and standards, VPN security standard, and wireless security policy documents to triangulate the data. I reviewed the firewall policy document, which contain the excerpt, "The purpose and objectives of this policy are to ensure that all access to critical systems, devices, and networks are validated by a firewall securely." I used the company documents to validate responses from the participants during the interviews. RP5 stated, "The management shows a big interest and knows the

importance of informing and educating the staff about security threats, preventive security standards, and policies addressing cyber threats." RP3 stated,

> Cybersecurity in a bank is essential. Therefore, we take this matter at the highest importance with our employees. We exercise a self-audit periodically to assure the validity of all internal procedures and that our customers' data are well maintained and safeguarded from any breach or leakage.

Elkhannoubi and Belasissaoui (2016) recommended that leaders develop a cybersecurity culture to help users of information systems protect the organization from harm. RP1 stated,

> We focus on the need for a stable security governance program to be in place, so we can plan, design, and implement all the needed security strategies and processes. Only with stable information security governance in place can an organization begin to address the threats to their survivability and profitability.

Cybersecurity must be a regular part of a company's governance arrangements (Scully, 2013). Corporate executives, managers, and cybersecurity professionals rely extensively on technology to avert cybersecurity incidents (Nobles, 2018). RP1 added,

> Protecting information systems from cyber threats is to direct and support the organization in the protection of their information assets from intentional or unintentional disclosure, modification, destruction, or denial through the implementation of appropriate information security and business planning policies, procedures, and guidelines.

RP2 stated, “Implementing a bank-wide security policy requires us to be precise and flexible to update security policies that we use as a vital road map for the bank information technology team to maintain an efficient adaptive security architecture.” A central responsibility of a business leader is to ensure that the development and maintenance of written policies and procedures related to cybersecurity (Blank et al., 2016; Herath et al., 2014).

A cybersecurity policy is a set of procedures issued by an organizational leader to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization’s boundaries of authority (Hewett et al., 2016). Business leaders employ information security policies to protect their digital assets and intellectual rights in efforts to prevent theft of industrial secrets and information that could benefit competitors (Bodin et al., 2018). All participants in this study recommended having a clear information security policy and procedure for every department as a strategy for protecting information systems from cyber threats. To secure information systems and protect organizational infrastructure, information technology professionals need to understand the critical elements of cybersecurity strategies and coordinate their efforts at local, national, and global levels (Kshetri & Murugesan, 2013).

Theme 3: Risk Management Strategy

The third major theme in this study was the topic of risk management. The risk management theme emerged from the responses of all research participants and my

review of company document. This finding confirms the research of Wilgus (2018) in that risk management is an essential and fundamental criterion in information security. Risk management is the process of identifying, assessing, and controlling threats to an organization's capital and earnings (Yang et al., 2017). Scholars attributed threats, or risks to a wide variety of sources, including cyberattacks, financial uncertainty, legal liabilities, strategic management errors, accidents, and natural disasters (Sheedy et al., 2017; Yang et al., 2017).

Freund (2018) noted that risk management is a process of recognizing, assessing, and mitigating risk. Brady (2018) stated that banks are risk management operations and are dependent on sophisticated technology spanning vast networks of branches and subsidiaries. I reviewed the acceptance usage, access control, antimalware and spam, backup, firewall, critical risk indicator report and areas of assessment, network security, password policy and standards, VPN security standard, and wireless security policy documents to triangulate the data. I reviewed the VPN security standards policy, which contained the excerpt, "Information technology risk department should verify the appropriateness of the request by validating the business purpose. Information technology risk should also perform a security risk analysis before approving any requests" to validate RP1's interview response. RP1 stated,

> We strive to identify and understand the principal risks acceptable to the organization in the pursuit of its strategy, develop our risk appetite, and establish and communicate the relevant control and reporting frameworks for each risk, including responsibilities, authorities, and key contributors. We establish a

> process for evaluating each risk, agree on a measurement approach and reporting standards, and develop measurement methodologies and models for assessment of internal and external risks.

Risk is an integrated evaluation that leaders use to ascertain how effective are the existing means of protecting bank information from cyberattacks (Hryshchuk & Yevseiev, 2016). The Company leaders use key risk indicators to verify the strength of the cybersecurity processes as part of their risk management strategy. RP2 stated,

> We enhance the cybersecurity culture by setting key performance indicators and key risk indicators to increase the awareness and the interest of the employees to comply with the institution's applied security framework and to report every month the key risk indicators to top management to make them aware of the bank information security risks.

RP5 stated, "We apply a key risk indicator to report the high-security risk incidents and cyber threats to the top management." According to the Company's Key Risk Indicator Report and Areas of Assessment document, management has outlined areas of risk assessment. I review the Key Risk Indicator Report and Areas of Assessment document. I created a matrix in Figure 2 to display the significant aspects of the document.

Area of assessment	Key risk indicator
Cyberattacks	Number of phishing attacks Number of denials of service attack attempts Number of Botnet discovered
Malware	Number of malwares detected and cleaned (host, email, internet-based malware)
Advanced persistent threats/ zero day attacks	Number of advanced persistent threats detected and blocked
Spam messages	Number of spam messages detected and blocked
System/network interiority breaches	Number of network breach attempts (port scans, unusual traffic) Number of system breaches attempts
Intrusion attempts	Number of host-based intrusion attempts Number of network-based intrusion attempts
Vulnerabilities	Number of new vulnerable systems identified

Figure 2. Key risk indicator and areas of assessment matrix.

Grobler (2018) noted that small financial institutions' stability remains dependent on reputation and risk mitigation. All participants noted that cybersecurity was an integral part of their risk management strategy. RP1 stated, "We developed and implemented an ongoing risk assessment program targeting information security and privacy matters, recommended methods for vulnerability detection and remediation, and oversee vulnerability testing internally and externally."

Research participants' responses were consistent on the concept of threat mitigation. Bozkus and Caliyurt (2018) suggested that the safest way to respond to cyber threats is to root the organization's cybersecurity strategy in their business strategy. Hryshchuk and Yevseiev (2016) acknowledged that threats to bank information security

that significantly affect the bank, bank staff, and its clients as well as on the economic component of national security are the internal and external threats. RP2 stated, "Like any other bank risk, cyber-risk should be subject to the general risk management principles of risk identification, control, monitoring, and mitigation." RP1 stated,

> Ensure that information created, acquired, or maintained by the institution, and its authorized users, is used in accordance with its intended purpose; to protect the institution information from external or internal threats; and to assure that it complies with statutory and regulatory requirements regarding information access, security, and privacy as well as industry best practices.

Ifinedo (2014) acknowledged in confronting emerging threats, and security and privacy concerns, a need exists for organizations and their workers to build consensus and foster relationships on these issues. RP4 stated, "We are applying the newest updates related to the information security against any cyberattacks or threats of any kind." RP3 stated,

> Our information technology department deals with external threats. To the best of my knowledge, the main internal procedures tailored to protect information systems from external cyber threats are updating antiviruses and firewalls to the latest available in the industry, systematic backup, disaster recovery plan, and strict compliance with the regulatory authority rules and regulations.

Academic scholars acknowledged that organizational leaders identify and evaluate risks to the confidentiality, integrity, and availability of their information assets (Shamala, Ahmad, Zolait, & Sedek, 2017). Ionut (2017) considered that risk management

is an iterative, ongoing process between the existing and desired security state, through the evaluation and management of risks. Information security risk management is the primary methods by which organizational leaders preserve the privacy, reliability, and availability of information resources (Webb, Ahmad, Maynard, & Shanks, 2014). In agreement with the findings in existing literature, the participants consistently stated that risk management strategy was a means to address confidentiality, integrity, and availability of the information system. All participants commented that information privacy, information availability, and cybersecurity were key considerations regarding their risk management strategy.

Theme 4: Organizational Strategy

The final major theme from my data analysis was organizational strategy. The organizational strategy theme emerged from the responses of four research participants as well as their supporting documentation. The research participants responded with subthemes to an organization-wide strategy, which were security strategy, information security strategy, successful business practice strategies, efficient strategy, and dynamic strategy. This finding supports the research of James (2018) who affirmed that an organization's security strategy aligns with business strategy and is an integral component of the senior leadership's decision-making process. RP5 stated, "Every organization and specifically the financial institutions should have an efficient cybersecurity and information systems strategy to protect their client's data, and their online banking applications by applying a cybersecurity strategy." RP1 stated,

> We developed an information security strategy in support of the business strategy and created the program in full view while working with the other components of the organization; the program must meet the needs of the organization and not just be an implementation of advanced controls.

I reviewed the network security policy, which contained the excerpt, "The Company's data processing architecture relies heavily on its network. Maintaining a secure network is essential to our success." The network security policy contained clear language regarding the security needed to protect data, processing, and communication facilities, all essential components of the Company's security environment. I used the network security policy to validate RP1 and RP5's interview responses.

Carías, Labaka, Sarriegi, and Hernantes (2019) stated an organizational strategy for cyber resilience should be dynamic, based on technical security and personnel training. Boiko, Shendryk, and Boiko (2019) affirmed that to develop an effective organizational cybersecurity strategy for financial institutions, leaders must understand the cybersecurity risk about the organization and critical business operations. RP3 acknowledged,

> To the best of my knowledge, the bank IT department is always following a dynamic strategy to keep the system secured with the latest available firewalls in the industry. There are specific regulatory standards set by Qatar Central Bank that we must comply with to remain in compliance.

Noting a way to develop an organizational strategy for cybersecurity, RP2 stated,

> I would encourage the updating of antivirus and antispyware software on every computer and patch all systems with the latest security patches and regularly update and upgrade the firewalls, antithreat programs, and hardware to protect the servers, the network, and our customer's data, and highly secure our online services.

An organizational strategy is the aggregate of actions a company leader intends to take to achieve long-term goals (Ocasio & Radoynovska, 2016). Allam Abu (2016) recommended that the organizational structure integrated with the company's strategy is a means for business leaders to achieve the organization's vision, mission, and goals towards strategies for protecting information systems. RP5 stated, "We have an agreement within an external specialized information security company to regularly conduct external penetration testing to our firewalls and security systems facing the public Internet and online applications to report about vulnerabilities." Researchers noted that organizational strategies must align with information security policies to be effective in protecting against cyber threats (Soltanizadeh, Abdul Rasid, Mottaghi Golshan, & Wan Ismail, 2016). All participants suggested implementing a strategy to combat and block any cybersecurity threat as part of the entire organization's strategy.

Findings Linked to the Conceptual Framework

The research findings were consistent with the significance of the study and related to Law's (1992) actor-network theory. The actor-network theory was a useful lens to explore the strategies used by leaders to protect information systems from cyber threats because of the ability to represent the heterogeneity of networks and human as well as

nonhuman actors to develop a new systematic process or change. The actor-network theory is a framework that leaders use to track the multipart interplay of humans and digital technology to give a focus on the relationship between nonhumans and humans that encapsulated the arbitrated nature of modern life within an evolved technological culture (Rocci, 2014). Researchers can use actor-network theory to explore the role of a heterogeneous network regarding influencing outcomes and determining the behavior of individuals in the network (Montenegro & Bulgacov, 2015). Researchers discussed the actor-network theory as a framework for analyzing sociotechnical processes and applying them to cybersecurity practices to surmise the causes of the lack of strategies by leaders to protect information systems within small financial institutions (Callon, 1986; Latour, 1986; Law, 1992).

Scholars used the actor-network theory with inanimate sources, making the theory a pragmatic approach to model the strategies leaders of small financial institutions used to protect information systems from cyber threats outside the human domain. The term *actor* denoted stakeholders, all of whom are aware of and respond to the entire network (Weaver, Ellen, & Mathiassen, 2015). Instead of treating information security, cybersecurity policy, risk management, and organizational strategy as separate entities, through the lens of the actor-network theory, the findings of this study indicate that leaders of the Company considered these strategies and tactics as a collective network to protect information systems from cyberattacks. Business leaders should take a holistic, systems approach regarding the protection of information systems (Sunday & Vera

Chinwedu, 2018). The actor-network theory was an essential part of my understanding the interconnected strategies leaders used to protect their information systems.

All themes that emerged from the analyzed played a crucial role in my understanding of the research topic and addressing the central research question. Each theme identified required heterogeneity of networks and human as well as nonhuman actors to develop a new systematic process or change between (a) information security management, (b) cybersecurity policy, (c) risk management, and (d) organizational strategy. The findings through the lens of actor-network theory resulted in a reduced gap in business knowledge regarding cybersecurity practices essential for small financial institutions to avoid potential data breaches.

Findings Linked to Existing Literature on Business Practice

The findings in this study were consistent with existing research literature regarding cybersecurity practices. The emerging themes in this study confirmed and aligned with the findings of Lucas (2018) and Maahs (2018) in that information security management, cybersecurity policy, risk management, and organizational strategy are practices leaders use to protect information systems from cyber threats. A properly developed information systems security plan should contain a cybersecurity policy, an organizational security strategy, a plan for security requirements, an outline the individual roles and responsibilities, a definition of the authorized and unauthorized system use, an outline of rules and protocols, the penalties for noncompliance, and a detailed plan for continuous monitoring, testing, and updating (Whitman, 2004). Lucas (2018) noted that leaders implemented effective information systems strategies by

identifying, assessing, and understand the risks and threats, installing up-to-date hardware and software, implementing detailed cybersecurity policies, and continuous monitoring of the information networks. Maahs (2018) found that organizational policies, information technology structure, managerial strategies, and assessment and actions were integral with developing cybersecurity best practices.

Applications to Professional Practice

All participants in this study agreed that information security management, cybersecurity policy, risk management, and organizational strategy were strategies used to protect information systems from cyber threats. The findings from this study may contribute to the body of knowledge regarding best practices to protect information systems within small financial institutions. Study participants were business leaders from a small financial institution in Doha, Qatar, who have successfully implemented strategies to protect information systems from cyber threats. The results may apply to other small businesses who are lacking strategies to information systems from cyber threats. Through the documentation of real-world leaders' practices regarding strategies to protect information systems, the findings of this study might result in business leaders improving their business practices through reductions in cyber threats.

Leaders could potentially apply the findings to develop and implement a robust information security management strategy to protect their information systems from cyber threats. Leaders might find this strategy useful to ensure the confidentiality, integrity, and availability of company data, such as customer records, proprietary documents, financial data, and internal memos. Leaders may then be able to create a

management process they use to identify assets, threat sources, vulnerabilities, risks, and effective network controls.

Cybersecurity policy strategy was the second theme that emerged from the analyzed data. The functions of a leader in a managerial role are to plan, lead, control, and organize the mission and vision of the organization (Terlizzi et al., 2017). Leaders of financial institutions might apply a cybersecurity strategy to guide expenditures and efforts toward building a more secure business environment. The cybersecurity policy was a document created by leaders to outlined specific requirements or protocols that meet the needs of an organization information system. Leaders may be able to apply the findings in this study to evaluate, create, or change organizational cybersecurity policy to ensure the protection of data, information systems, and internally and externally used networks.

Risk management strategy was the third theme that emerged from the interview and document data. Leaders of organizations must be able to identify the potential risk or vulnerabilities that may affect the data of the organizations (Iverson & Terry, 2018). To understand the risk that may affect an organization information system, leaders need to have all the right information to make the best decisions. Based on the participant's responses, their organization goes through weekly risk assessments to ensure proper protection of data. Leaders of financial institutions might apply the findings of this study to implement a risk management strategy to protect information systems from cyber threats. A risk management strategy would potentially be a means for business leaders to

validate the strength of their existing risk management policy and make upgrades as needed to ensure regulatory compliance and the protection of company data.

The last emerging theme from the analyzed data was an organizational strategy. An organizational strategy is the sum of the actions company leaders intend to take to achieve long-term goals (Rothrock et al., 2018). Leaders of financial institutions should implement a holistic organizational strategy if they are to mitigate the cyber risks to their information systems (Camillo, 2017). Leaders might apply the findings of this study to implement a holistic, systemic organizational strategy to ensure the protection of information systems from cyber threats. Leaders may find the information regarding organization strategy useful to develop tools and resources to examine and revise existing organizational strategies.

Small financial institutions with insufficient security budgets and inadequate data protection remain at risk for cyberattacks. Small financial institutions lack the resources, finances, and security infrastructure that larger organizations employ to prevent or mitigate cyberattacks (Harris & Patten, 2014). Business leaders in the financial sector might improve their business practices by implementing effective strategies used in the protection of small financial institutions' information systems from cyber threats and data breaches.

Implications for Social Change

Leaders of financial institutions might use the findings of this study to affect positive social change through decreasing data breach occurrences, safeguarding the confidential information of consumers, and reducing the risk and costs of consumer

identity theft. Leaders of small financial institutions might improve the protection of consumer data and reduce the cost associated with consumer identity theft by implementing the recommendations from this study. Effective organizational leaders use technologically advanced digital privacy to implement positive social change, reduce consumers' exposure to security breaches, and improve community engagement (Jewkes & Yar, 2011). To counter the evolving cyber threat facing organizations, business leaders must ensure they have an integrated approach to cybersecurity tailored to their business and risk profile, addressing not only the technical aspects of their defense, but also the human, organizational, and societal elements (Nevmerzhitskaya, Norvanto, & Virag, 2019).

Galinec, Možnik, and Guberina (2017) stated that cybersecurity encompassed a broad range of practices, tools, and concepts related closely to information and operational technology security that business leaders use to protect consumer data. Casesa (2019) acknowledged an effective cybersecurity strategy results in reduced exposure to cyber threats and improved protection of consumer information. To reduce the cost to consumers, business leaders need to recognize the best strategies to decrease the occurrences of data security breaches. Eighty-one percent of data security breaches occur because of consumer data theft (Lai et al., 2012). Enlightening business leaders of the plan on ways of thwarting and alleviating cyber threats may aid in business growth and profitability for expanding organizations' support for societies (Cant & Wiid, 2013; Coetzee et al., 2013). Small financial institution leaders can minimize the exposure of

their network systems from cyberattacks with the creation and implementation of effective strategies.

Recommendations for Action

My objective in this qualitative study was to understand and explore what strategies leaders of a small financial institution used to protect information systems from cyber threats in Doha, Qatar. Four themes emerged from my data analysis: information security management, cybersecurity policy, risk management, and organizational strategy. Information security policies are the foundation of an effective cybersecurity program. With defined information security policies, individuals will understand the *who, what,* and *why* regarding their organization's security program as well as the need for organizational risk mitigation. I recommend leaders of financial institutions use an information security management strategy to (a) protect their organizations, employees, customers, vendors, and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information; (b) protect the integrity of the information; (c) ensure the availability of information through effective systems management; (d) understand the role of security policies in their organizations; (e) ensure the enforceability of security policies; and (f) explain how to handle policy exceptions.

Leaders might consider implementing an information security management strategy to effectively plan, lead, control, and organize security to protect information systems.

I recommend that leaders develop and implement robust cybersecurity strategies. A cybersecurity strategy along with detailed policies might be of benefit to employees

regarding how to use information technology in the workplace in a safe manner. Cybersecurity is a set of techniques used to protect the integrity of networks, programs, and data from attack, damage, or unauthorized access (Gonzalez-Granadillo et al., 2018). I recommend that leaders of organizations examine and assess existing cybersecurity policies using the findings of this study to:

- Identify critical assets and threats
- Prioritize risks and threats
- Set achievable goals.

Risk management is a fundamental principle of cybersecurity (Prince, 2018). Cyber risks are risk of financial loss, disruption, or damage to the reputation of an organization from some failure of the information technology systems (Prince, 2018). I recommend the following actions by leaders to follow when developing risk management strategies: (a) understand the cybersecurity risk about the organization and critical business operations; (b) integrate the strategy across personnel, technical security, information assurance, and physical security; (c) establish protective monitoring to prevent and deter internal and external threats; and (d) accept that some cyberattacks will breach the business defense and plan on this basis.

The final theme that emerged in this study was an organizational strategy. Based on the results of this study, I recommend that leaders of financial institutions develop a holistic, systemic organizational strategy regarding cybersecurity. Leaders of financial institutions lacking a systemic, organizational approach to cybersecurity are unlikely to protect their information systems with adequate security measures (Camillo, 2017).

Organizational leaders implement a holistic strategy to ensure the security of their information systems and attain long-term sustainability and success (Rothrock et al., 2018). I also recommend that leaders consider using an organization strategy to engage in effective cybersecurity practices, protect their information systems, and mitigate the effects of data breaches.

I plan to disseminate the findings of this study by providing the participants with an executive summary of the results. I intend to submit articles for publication in the *Journal of Risk Management in Financial Institutions* and the *Journal of Cyber Security and Information Systems.* I will seek opportunities to present the findings at financial or information security workshops and conferences, such as the *International Conference on Economics Finance and Accounting* in Qatar.

Recommendations for Further Research

I conducted a qualitative, single case study, collecting data from five leaders of one financial institution in Qatar. Limitations exist in this study because of the research method and design as well as the geographic location. I recommend that researchers conduct further studies to address the assumptions, limitations, and delimitations outlined in this study. Future researchers could conduct a mixed-method research study to explore strategies leaders used to defend against cyber threats in tandem with testing models or creating new theory to expand the existing body of knowledge. A future researcher might consider conducting a quantitative, correlational study to examine the relationship among variables, such as information security breaches, cost of information security, consumer confidence in the financial system, and effective network solutions to reduce cyber

threats. Future researchers could use a qualitative, multiple case study design to expand the scope of this single case study and gain additional insight into leaders' knowledge of how to protect information systems from cyber threats. Researchers collecting data from leaders of multiple companies might reveal additional strategies for protection of information systems, leading to the implementation of more effective business practices in the banking and financial industries.

I recommend further research on the lack of information security policies in a different geographic location to overcome a limitation of this study. A researcher in a different geographic location might reveal strategies undiscovered by my research because of different levels of threat, regulatory and compliance issues, consumer privacy laws; therefore, potentially allowing leaders of small financial institutions who lack effective strategies the added insight needed to adopt effective cybersecurity policies. Researchers in different locations or industries could investigate the applicability of the conclusions and transferability of the findings of this study to other business contexts. Future researchers might consider using the actor-network theory in combination with other theories to develop a conceptual model regarding cybersecurity strategies. Gasca-Hurtado and Losada (2013) noted that researchers could actor-network theory in combination with other social theories to provide new insight into complex information systems projects. Other social theories, such as complex adaptive systems theory and structured theory to explore decision-making and network actors might prove beneficial to future researchers as well as information security leaders.

Reflections

I started my doctoral journey in 2009. When I started the DBA program, I did not know how rigorous the process would be to complete. I was unsure about my topic because as a business leader, I wanted to conduct beneficial research, but did not want to research a topic that might create risk or challenges for participants or the research partner organization. I also wanted to research a topic that would provide value to the nation of Qatar. I started reading local periodicals when I came up with my research topic. In 2022, Qatar will be hosting the FIFA World Cup Soccer tournament. With this being a global event, many tourists will be visiting Qatar during this 30-day soccer event. Central concerns of local business leaders are if the financial system is able to handle all the daily transaction of individuals and how safe is the country from cyberattacks? With this information, I gleaned a research topic that might result in a positive social effect for Qatar.

After selecting this topic and obtaining approval from Walden University IRB, a significant challenge I faced was finding participants. I learned that many financial institutional leaders are not willing to allow an outside individual to come into their organization and research their information security strategies and policies. I had to develop a working relationship with the participants by purposely connecting with them through emails and in person, having responsibility as the research to the participants. Developing a working relationship with participants in this study was critical for success. Once I was able to secure a research site and participants, I felt this was a victorious moment.

The first joyous moment in my doctoral journey was finally receiving approval of the proposal. I worked extremely hard to write my proposal based on the requirements of Walden University. I express my gratitude to my chair and committee for their guidance. The challenges of completing my doctoral study were time management and motivating myself to write. Many times, I became discouraged because of the feedback I received regarding submissions of my study. The way I overcame these challenges was imagining the day when I finally walk across the stage to receive my degree.

I enjoyed the journey of completing this DBA degree. I was able to see the growth I achieved as a researcher and practitioner from the start of the program to the point I completed my study. I am grateful to have had the opportunity to research a topic that will have an immediate effect on the banking industry of Qatar, and on increasing the awareness of business leaders to take the necessary measures to protect their information system and data from cyber threats and attacks through their applied strategies.

Conclusion

The purpose of this qualitative, single case study was to explore the strategies leaders of a small financial institution used to protect information systems from cyber threats. The actor-network theory was the conceptual framework for this study. I purposefully selected five leaders of a small financial institution based in Doha, Qatar as participants. I collected data from semistructured, face-to-face interviews, and a review of company documents. Using Yin's 5-step data analysis process, the four themes emergent themes were information security management, cybersecurity policy, risk management, and organizational strategy. The findings of this study indicate that leaders of financial

institutions protect their information systems from cyber threats through effective management of information security practices, developing robust cybersecurity policies, identifying, assessing, and mitigating cybersecurity risks, and implementing a holistic organizational strategy. The protection of information systems through reductions in cyber threats by leaders can improve their organizational business practices. Leaders of financial institutions might use the findings of this study to affect positive social change through decreasing data breach occurrences, safeguarding the confidential information of consumers, and reducing the risk and costs of consumer identity theft.

References

Abdul-Wahab, A., & Haron, R. (2017). Efficiency of Qatari banking industry: An empirical investigation. *International Journal of Bank Marketing*, *35*, 298–318. doi:10.1108/IJBM-07-2016-0090

Adaba, G. B., & Ayoung, D. A. (2017). The development of a mobile money service: An exploratory actor-network study. *Information Technology for Development*, *23*, 668–686. doi:10.1080/02681102.2017.1357525

Afzaal, H., & Zafar, N. (2016). Formal analysis of subnet-based failure recovery algorithm in wireless sensor and actor and network. *Complex Adaptive Systems Modeling*, *4*(1), 1–27. doi:10.1186/s40294-016-0037-4

Ahmad, A., Maynard, S. B., & Park, S. (2012). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*, 357–370. doi:10.1007/s10845-012-0683-0

Ahmed Shareef, Z., Hughes, R., & Petridis, M. (2014). Exposing the influencing factors on software project delay with actor-network theory. *Electronic Journal of Business Research Methods*, *12*, 132–146. Retrieved from http://www.academic-conferences.org/ejournals.htm

Akgun, A. E., Keskin, H., & Byrne, J. C. (2014). Complex adaptive systems theory and firm product innovativeness. *Journal of Engineering and Technology Management*, *31*, 21–42. doi:10.1016/j.jengtecman.2013.09.003

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, *74*, 323–339. doi:10.1016/j.cose.2017.09.011

Alby, F., & Fatigante, M. (2014). Preserving the respondent's standpoint in a research interview: Different strategies of 'doing' the interviewer. *Human Studies*, *37*, 239–256. doi:1007/s10746-013-9292-y

Al-Hamar, A. K. (2016). Enhancing information security process in organizations in Qatar. *Qatar Foundation Annual Research Conference Proceedings*, 2016(1), p. ICTPP2531. doi:10.5339/qfarc.2016.ICTPP2531

Alex da, M. P., Näslund, D., & Jasmand, C. (2012). Logistics case study based research: Towards higher quality. *International Journal of Physical Distribution & Logistics Management*, *42*, 275–295. doi:10.1108/09600031211225963

Ali, L. (2019). Cybercrimes—a constant threat for the business sectors and its growth (a study of the online banking sectors in GCC). *Journal of Developing Areas*, *53*, 267–279. doi:10.1353/jda.2019.0016

Allam Abu, F. (2016). Matching organizational frame of reference and business strategy with contemporary marketing practices: Evidence from Arab world. *International Journal of Emerging Markets*, *11*, 533–549. doi:10.1108/IJoEM-05-2015-0104

Ananda Kumar, V., Pandey, K. K., & Punia, D. K. (2014). Cybersecurity threats in the power sector: Need for a domain-specific regulatory framework in India. *Energy Policy*, *65*, 126–133. doi:10.1016/j.enpol.2013.10

Ananthasubramanian, U. (2018). Regulatory, technological, and human resource challenges for enhancing effectiveness of Indian banks. *Vinimaya, 38*, 11–21. Retrieved from http://www.nibmindia.org/

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

Anderson, K. (2017). Using agility to combat cyberattacks. *Journal of Business Continuity & Emergency Planning, 10*, 298–307. Retrieved from http://www.henrystewartpublications.com/

Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a codebook. *Comprehensive Psychology, 3*, 1–7. doi:10.2466/03.CP.3.4

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

Applebaum, L. (2014). From whining to wondering: Reflective journaling with preservice educators. *Journal of Jewish Education, 80*(1), 5–23. doi:10.1080/15244113.2014.880140

Atoum, I., & Otoom, A. (2016). Effective belief network for cybersecurity frameworks. *International Journal of Security and Its Applications, 10*, 221–228. doi:10.14257/ijsia.2016.10.4.21

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

Balzacq, T. (2014). The significance of triangulation to critical security studies. *Critical Studies on Security*, *3*, 377–381. doi:10.1080/21624887.2014.982410

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security, 1*, 176–198. doi:10.1017/eis.2016.8

Banham, R. (2017). Cybersecurity: A new engagement opportunity: An AICPA framework enables CPAs with cybersecurity expertise to perform new services for clients. *Journal of Accountancy*, *224*(4), 28–32. Retrieved from http://www.aicpa.org/Pages/default.aspx

Barasa, E. W., Molyneux, S., English, M., & Cleary, S. (2017). Hospitals as complex adaptive systems: A case study of factors influencing priority setting practices at the hospital level in Kenya. *Social Science & Medicine*, *174*, 104–112. doi:10.1016/j.socscimed.2016.12.026

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

Baškarada, S. (2014). Qualitative case study guidelines. *Qualitative Report, 19*, 1–18. Retrieved from http://www.nova.edu/tqr/

Bazzano, M. (2014). On becoming no one: Phenomenological and empiricist contributions to the person-centered approach. *Person-Centered & Experiential Psychotherapies*, *13*, 250–258. doi:10.1080/14779757.2013.804649

Bedwell, C., McGowan, L., & Lavender, D. T. (2015). Factors affecting midwives' confidence in intrapartum care: A phenomenological study. *Midwifery*, *31*(1), 170–176. doi:10.1016/j.midw.2014.08.004

Bell, S. (2017). Cybersecurity is not just a 'big business' issue. *Governance Directions*, *69*, 536–539. Retrieved from http://www.copyright.com.au

Benmamoun, M., Sobh, R., Singh, N., & Moura, F. T. (2016). Gulf Arab e-business environment: Localization strategy insights. *Thunderbird International Business Review*, *58*, 439–452. Retrieved from https://onlinelibrary.wiley.com/journal/15206874

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

Berger, R. (2015). Now I see it; now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research*, *15*, 219–234. doi:10.1177/1468794112468475

Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches* (2nd ed.). Thousand Oaks, CA: Sage.

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

Bhattacharya, S. (2014). Institutional review board and international field research in conflict zones. *PS, Political Science & Politics, 47*, 840–844. doi:10.1017/S1049096514001140

Blank, T. C., Kohlhofer, D. B., & Bonaccorsi, H. (2016). Regulatory monitor. *Investment Lawyer*, *23*, 28–30. Retrieved from http://www.aspenpublishers.com

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research, 19*, 426–432. doi:10.1108/QMR-06-2016-0053

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*, 527–544. doi:10.1016/j.jaccpubpol.2018.10.004

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks, and cyber security. *Procedia Computer Science*, *2019*(149), 65–70. Retrieved from https://www.journals.elsevier.com/procedia-computer-science

Bölte, S. (2014). The power of words: Is qualitative research as important as quantitative research in the study of autism? *Autism*, *18*, 67–68. doi:10.1177/1362361313517367

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law, and Social Change, 67*, 265–288. doi:10.1007/s10611-016-9653-3

Bowers, T. (2018). Heterotopia and actor-network theory: Visualizing the normalization of remediated landscapes. *Space & Culture*, *21*, 233–246. doi:10.1177/1206331217750069

Bozkus, K. S., & Caliyurt, K. (2018). Cybersecurity assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360–376. doi:10.1108/MAJ-02-2018-1804

Bradley, P. V., Getrich, C. M., & Hannigan, G. G. (2015). New Mexico practitioners' access to and satisfaction with online clinical information resources: An interview study using qualitative data analysis software. *Journal of the Medical Library Association, 103,* 31–35. doi:10.3163/1536-5050.103.1.006

Brady, S. (2018). Banks lead the fight against cyber risk. *Euromoney*, *49*(589), 60. Retrieved from https://www.euromoney.com/

Brayda, W. C., & Boyce, T. D. (2014). So, you really want to interview me? Navigating "sensitive" qualitative research interviewing. *International Journal of Qualitative Methods*, *13*, 318–334. Retrieved from http://globalsecuritystudies.com/vol5iss3summer2014.htm

Brooks, L., Atkinson, C., & Wainwright, D. (2008). Adapting structuration theory to understand the role of reflexivity: Problematization, clinical audit, and

information systems. *International Journal of Information Management*, *28*, 453–460. doi:10.1016/j.ijinfomgt.2008.08.009

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford, United Kingdom: Oxford University Press.

Burley, D. L. (2018). Managing cybersecurity risk in the age of "smart" everything. *Information Systems Security Association Journal, 16*(2), 7–24. Retrieved from http://www.issa.org/

Callon, M. (1986). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieux Bay. In J. Law (Ed.), *Power, 253 section and relief exobiology of knowledge?* (pp. 196–229). London, United Kingdom: Routledge and Kegan Paul.

Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions, 10*, 196–200. Retrieved from https://www.henrystewartpublications.com/jrm

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

Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a cyber resilience investment strategy in an industrial internet of things context. *Sensors, 19*(1), 138–154. doi:10.3390/s19010138

Casesa, P. (2019). Bridging the cyber gap: Spotting hidden security talent in your organization. *Information Systems Security Association Journal*, *17*(2), 18–23. Retrieved from http://www.issa.org/

Castleberry, A. (2014). NVivo 10 [software program]. Version 10. QSR International, 2012. *American Journal of Pharmaceutical Education, 78,* 25–26. doi:10.5688/ajpe78125

Cavalheiro, G. C., & Joia, L. A. (2016). Examining the implementation of a European patent management system in Brazil from an actor-network theory perspective. *Information Technology for Development*, *22*, 220–241. doi:10.1080/02681102.2014.910634

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

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

Chittem, M. (2014). Understanding coping with cancer: How can qualitative research help? *Journal of Cancer Research & Therapeutics, 10,* 6–10. doi:10.4103/0973-1482.131328

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organizational insiders. *Journal of Information Science, 44*, 752–767. doi:10.1177/0165551517748288

Choucri, N., Madnick, S., & Ferwerda, J. (2013). Institutions for cybersecurity: International responses and global imperatives. *Information Technology for Development, 20*, 96–121. doi:10.1080/02681102.2013.836699

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

Comizio, V. G., Dayanim, B., & Bain, L. (2016). Cybersecurity as a global concern in need of global solutions: An overview of financial regulatory developments in 2015. *Journal of Investment Compliance, 17*, 101–111. doi:10.1108/JOIC-012016-0003

Coole, M., & Brooks, D. J. (2014). Do security systems fail because of entropy? *Journal of Physical Security, 7*, 50–76. Retrieved from http://www.anl.gov/

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

Copeland, M. (2017). Cybersecurity: How security vulnerabilities affect your business. *Cyber Security on Azure*, 3–31. doi:10.1007/978-1-4842-2740-4_1

Cox, D. D., & McLeod, S. (2014). Social media marketing and communications strategies for school superintendents. *Journal of Educational Administration, 52*, 850–868. doi:10.1108/JEA-11-2012-0117

Cridland, E. K., Jones, S. C., Caputi, P., & Magee, C. A. (2014). Qualitative research with families living with autism spectrum disorder: Recommendations for

conducting semistructured interviews. *Journal of Intellectual and Developmental Disability, 40*, 78–91. doi:10.3109/13668250.2014.964191

Christo, C., Dewald, V. N., & Emmanuel, R. (2016). Disaster resilience and complex adaptive systems theory: Finding common grounds for risk reduction. *Disaster Prevention and Management, 25*, 196–211. doi:10.1108/DPM-07-2015-0153

Cugini, M. (2015). Successfully navigating the human subjects approval process. *Journal of Dental Hygiene, 89*, 54–56. Retrieved from http://jdh.adha.org

Cummings, J. A., Zagrodney, J. M., & Day, T. E. (2015). Impact of open data policies on consent to participate in human subjects' research: Discrepancies between participant action and reported concerns. *PLOS One, 10*, 1–11. doi:10.1371/journal.pone.0125208

Damghanian, H., Zarei, A., & Siahsarani Kojuri, M. A. (2016). Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran. *Journal of Internet Commerce, 15*, 214–238. doi:10.1080/15332861.2016.1191052

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Impacts of security climate on employees' sharing of security advice and troubleshooting: Empirical networks. *Business Horizons, 59*, 571–584. doi:10.1016/j.bushor.2016.07.003

Darnell, S. C., Giulianotti, R., Howe, P. D., & Collison, H. (2018). Reassembling sport for development and peace through actor-network theory: Insights from Kingston, Jamaica. *Sociology of Sport Journal, 35*, 89–97. doi:10.1123/ssj.2016-0159

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

Dawson, J., & Jöns, H. (2018). Unravelling legacy: A triadic actor-network theory approach to understanding the outcomes of mega events. *Journal of Sport & Tourism, 22,* 43–65. doi:10.1080/14775085.2018.1432409

De Albuquerque, J. P., & Christ, M. (2015). The tension between business process modelling and flexibility: Revealing multiple dimensions with a sociomaterial approach. *The Journal of Strategic Information Systems, 24,* 189–202. doi:10.1016/j.jsis.2015.08.003

De Ceunynck, T., Kusumastuti, D., Hannes, E., Janssens, D., & Wets, G. (2013). Mapping leisure shopping trip decision making: Validation of the CNET interview protocol. *Quality & Quantity, 47,* 1831–1849. doi:10.1007/s11135-011-9629-4

Denzin, K. N. (2012). Triangulation 2.0. *Journal of Mixed Methods Research, 6,* 80–88. doi:10.1177/1558689812437186

Doody, O., & Doody, C. M. (2015). Conducting a pilot study: Case study of a novice researcher. *British Journal of Nursing, 24,* 1074–80. doi:10.12968/bjon.2015.24.21.1074

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal, 72,* 538–562. doi:10.1177/0020702017741909

Dumay, J., & Rooney, J. (2016). Numbers versus narrative: An examination of a controversy. *Financial Accountability & Management*, *32*, 202–231. doi:10.1111/faam.12086

Dutta, D. K., Malhotra, S., & Zhu, P. (2016). Internationalization process, impact of slack resources, and role of the CEO: The duality of structure and agency in evolution of cross-border acquisition decisions. *Journal of World Business*, *51*, 212–225. Retrieved from https://www.journals.elsevier.com/journal-of-world-business

Edwards-Jones, A. (2014). Qualitative data analysis with NVIVO. *Journal of Education for Teaching*, *40*, 193–195. doi:10.1080/02607476.2013.866724

Elkhannoubi, H., & Belasissaoui, M. (2016). A framework for an effective cybersecurity strategy implementation. *Journal of Information Assurance & Security*, *11*(4), 233–241. Retrieved from http://www.mirlabs.org/jias

Erlingsson, C., & Brysiewicz, P. (2013). Orientation among multiple truths: An introduction to qualitative research. *African Journal of Emergency Medicine*, *3*(2), 92–99. doi:10.1016/j.afjem.2012.04.005

Essary, M. L. (2014). Key external factors influencing successful distance education programs. *Academy of Educational Leadership Journal*, *18*, 121–136. Retrieved from http://www.alliedacademies.org

Eze, S. C., & Chinedu-Eze, V. C. (2018). Strategic roles of actors in emerging information communication technology (EICT) adoption in SMEs. *Bottom Line: Managing Library Finances*, *31*, 114–136. doi:10.1108/BL-09-2017-0029

Fakhri, B., Fahimah, N., & Ibrahim, J. (2015). Information security aligned to enterprise management. *Middle East Journal of Business*, *10*, 62–66. Retrieved from http://www.mediworld.com.au

Farzan, F., Lahiri, S., Kleinberg, M., Gharieh, K., Farzan, F., & Jafari, M. (2013). Microgrids for fun and profit: The economics of installation investments and operations. *IEEE Power and Energy Magazine*, *11*, 52–58. doi:10.1109/mpe.2013.2258282

Federal Bureau of Investigation. (2015). *Internet Crime Complaint Center (IC3), 2014 IC3 annual report*. Retrieved from https://www.ic3.gov/media/annualreports.aspx

Feng, C., & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, *32*, 59–75. doi:10.1016/j.accinf.2018.11.001

Fidan, T. (2017). Managing schools as complex adaptive systems: A strategic perspective. *International Electronic Journal of Elementary Education*, *10*(1), 11-26. doi:10.26822/iejee.2017131883

Fidan, T., & Balci, A. (2017). Managing schools as complex adaptive systems: A strategic perspective. *International Electronic Journal of Elementary Education*, *10*, 11-26. Retrieved from https://eric.ed.gov/?id=EJ1156312

Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. *Games*, *9*, 34-37. doi:10.3390/g9020034

Fiske, S. T., & Hauser, R. M. (2014). Protecting human research participants in the age of big data. *Proceedings of the National Academy of Sciences, 111*, 13675-13676. doi:10.1073/pnas.1414626111

Flowers, A., Zeadally, S., & Murray, A. (2013). Cybersecurity and US legislative efforts to address cybercrime. *Journal of Homeland Security & Emergency Management, 10*(1), 1-27. doi:10.1515/jhsem-2012-0007

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

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development, 91*, 184-194. doi:10.1002/j.1556-6676.2013.00085.x

Freund, J. (2018). The future of IT risk management will be quantified risk. *Information Systems Security Association Journal, 16*(12), 10-16. Retrieved from http://www.issa.org/

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

Gai, K., Qiu, M., & Sun, X. (2018). A survey on Fintech. *Journal of Network & Computer Applications, 103*, 262-273. doi:10.1016/j.jnca.2017.10.011

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defense: National level strategic approach. *Automatika: Journal for Control, Measurement,*

Electronics, Computing & Communications, *58*, 273-286. doi:10.1080/00051144.2017.1407022

Gallagher, H., McMahon, W., & Morrow, R. (2014). Reports: Cybersecurity: Protecting the resilience of Canada's financial system. *Financial System Review*, 47-53. Retrieved from http://www.bankofcanada.ca/en/fsr/index.html

Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, *235*, 277-300. doi:10.1007/s10479-015-1925-2

Garfield, S., Hibberd, R., & Barber, N. (2013). English community pharmacists' experiences of using electronic transmission of prescriptions: A qualitative study. *BMC Health Services Research*, *13*(1), 1-26. doi:10.1186/1472-6963-13-435

Gargon, E., Gurung, B., Medley, N., Altman, D. G., Blazeby, J. M., Clarke, M., & Williamson, P. R. (2014). Choosing important health outcomes for comparative effectiveness research: A systematic review. *PLOS One, 9*, e99111. doi:10.1371/journal.pone.0099111

Gårseth-Nesbakk, L., & Kjærland, F. (2016). Precarious investments and blame gaming: Adverse effects and the inherent danger of simplification. *Financial Accountability & Management*, 3*2*, 281-308. doi:10.1111/faam.12097

Gasca-Hurtado, G. P., & Losada, B. M. (2013). Taxonomía de riesgos de outsourcing de software [Software outsourcing risk taxonomy]. *Chilean: Chilean Journal of Engineering, 21*(1), 41-53. Retrieved from http://www.scielo.cl/scielo.php/

Ghazzawi, A., Kuziemsky, C., & O'Sullivan, T. (2016). Using a complex adaptive system lens to understand family caregiving experiences navigating the stroke rehabilitation system. *BMC Health Services Research, 16*, 1-10. doi:10.1186/s12913-016-1795-6

Giblin, A. (2015). Insurance is an important tool in cyber risk mitigation. *Risk Management Association Journal, 97*, 32-37. Retrieved from https://www.rmahq.org/thermajournal/

Gill, M. J. (2014). The possibilities of phenomenology for organizational research. *Organizational Research Methods, 17*, 118-137. doi:10.1177/1094428113518348

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods, 16*, 15-31. doi:10.1177/1094428112452151

Gonzalez-Granadillo, G., Dubus, S., Motzek, A., Garcia-Alfaro, J., Alvarez, E., Merialdo, M., … Debar, H. (2018). Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems, 83*, 535-552. doi:10.1016/j.future.2017.05.043

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity, 1*, 3-17. doi:10.1093/cybsec/tyv011

Griggs, G., & Gul, S. (2017). Cybersecurity threats: What retirement plan sponsors and fiduciaries need to know-and do. *Journal of Pension Benefits, 24*, 17-21. Retrieved from http://www.aspenpublishers.com/

Grobler, J. (2018). Cyber risk from a chief risk officer perspective. *Journal of Risk Management in Financial Institutions, 11*(2), 125. Retrieved from https://www.henrystewartpublications.com/jrm

Gunawong, P., & Gao, P. (2017). Understanding e-government failure in the developing country context: a process-oriented study. *Information Technology for Development, 23*(1), 153-178. doi:10.1080/02681102.2016.1269713

Haahr, A., Norlyk, A., & Hall, E. O. (2014). Ethical challenges embedded in qualitative research interviews with close relatives. *Nursing Ethics, 21*, 6-15. doi:10.1177/0969733013486370

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*, 155-176. doi:10.1108/09685221111153546

Hanson, J. L., Balmer, D. F., & Giardino, A. P. (2011). Qualitative research methods for medical educators. *Academic Pediatrics, 11*, 375-386. doi:10.1016/j.acap.2011.05.001

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*, 97-114. doi:10.1108/IMCS-03-2013-0019

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*, 61-84. doi:10.1111/j.1365-2575.2012.00420.x

Hewett, R., Kijsanayothin, P., Bak, S., & Galbrei, M. (2016). Cybersecurity policy verification with declarative programming. *Applied Intelligence*, *45*(1), 83-95. doi:10.1007/s10489-015-0749-8

Higginbottom, G., Rivers, K., & Story, R. (2014). Health and social care needs of Somali refugees with visual impairment (VIP) living in the United Kingdom: A focused ethnography with Somali people with VIP, their caregivers, service providers, and members of the Horn of Africa Blind Society. *Journal of Transcultural Nursing*, *25*, 192-201. doi:10.1177/1043659613515715

Hill, A., & Bundy, A. C. (2014). Reliability and validity of a new instrument to measure tolerance of everyday risk for children. *Child: Care, Health, & Development*, *40*, 68-76. doi:10.1111/j.1365-2214.2012.01414.x

Hopkinson, G. C. (2017). Making a market for male dairy calves: Alternative and mainstream relationality. *Journal of Marketing Management*, *33*, 556-579. doi:10.1080/0267257X.2017.1301533

Höring, D., Gründl, H., & Schlütter, S. (2016). Impediments to communication in financial institutions: Implications for the risk management organization. *Geneva Risk & Insurance Review*, *41*, 193-224. doi:10.1057/s10713-016-0015-y

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case study research. *Nurse Researcher*, *20*(4), 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Hryshchuk, R., & Yevseiev, S. (2016). The synergetic approach for providing bank information security: The problem formulation. *Ukrainian Scientific Journal of Information Security, 22*(1), 64-74. Retrieved from http://jrnl.nau.edu.ua/

Ifinedo, P. (2014). The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management, 12*(2), 75-89. Retrieved from http://ijebm.ie.nthu.edu.tw/IJEBM_Web/index.htm

Ionut, R. (2017). Risk management from the information security perspective. *Junior Scientific Researcher, 3*(2), 1-8. Retrieved from https://www.jsrpublishing.com/

Iskandarova, M. (2017). From the idea of scale to the idea of agency: An actor-network theory perspective on policy development for renewable energy. *Science & Public Policy, 44*, 476-485. doi:10.1093/scipol/scw075

Iyamu, T., & Mgudlwa, S. (2018). Transformation of healthcare big data through the lens of actor-network theory. *International Journal of Healthcare Management, 11*, 182-192. doi:10.1080/20479700.2017.1397340

Iverson, A., & Terry, P. (2018). Cybersecurity hot topics for closely held businesses. *Journal of Pension Benefits: Issues in Administration, 25*, 60-62. Retrieved from http://www.aspenpublishers.com/

Jackson, A., Saffell, D. P., & Fitzpatrick, B. D. (2016). The evolving financial services industry: The financial advisory role today and in the future. *Journal of Business Inquiry: Research, Education & Application, 15*(1), 17-32. Retrieved from http://www.uvu.edu/woodbury/jbi/

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

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy, 5*, 87-88. doi:10.4103/0976-0105.141942

Jewkes, Y., & Yar, M. (2011). *Handbook of internet crime*. New York, NY: Routledge.

Jihoon, K., Kyoung-Yun, K., & Ohbyung, K. (2015). Actor-network theory-based modeling for crowdsourced design team formation. *Journal of Integrated Design & Process Science, 19*, 37-61. doi:10.3233/jid-2015-0010

Kache, F., & Seuring, S. (2014). Linking collaboration and integration to risk and performance in supply chains via a review of literature reviews. *Supply Chain Management, 19*, 664-682. doi:10.1108/SCM-12-2013-0478

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

Khan, S. N. (2014). Qualitative research method: Grounded theory. *International Journal of Business & Management, 9*, 224-233. doi:10.5539/ijbm.v9n11p224

Kim, J. (2017). Cyber-security in government: Reducing the risk. *Computer Fraud & Security*, *2017*(7), 8-11. doi:10.1016/S1361-3723(17)30059-3

Korhonen, J. J. (2014). Big data: Big deal for organization design? *Journal of Organization Design, 3*, 31-36. doi:10.146/jod.3.1.13261

Korte, J. (2017). Mitigating cyber risks through information sharing. *Journal of Payments Strategy & Systems*, *11*, 203-214. Retrieved from http://www.henrystewartpublications.com/

Kshetri, N. (2016). Cybersecurity in gulf cooperation council economies. *The Quest to Cyber Superiority*, 183-194. doi:10.1007/978-3-319-40554-4_11

Kshetri, N., & Murugesan, S. (2013). EU and US cybersecurity strategies and their impact on businesses and consumers. *Computer*, *46*(10), 84-88. doi:10.1109/MC.2013.350

Kshetri, N., & Voas, J. (2017). Banking on availability. *Computer*, *50*, 76-80. doi:10.1109/MC.2017.22

Kurokawa, M., Schweber, L., & Hughes, W. (2017). Client engagement and building design: The view from actor–network theory. *Building Research & Information, 45*, 910-925. doi:10.1080/09613218.2016.1230692

Latour, B. (1986). The powers of association. In J. Law (Ed.), *Power, action, and relief new sociology of knowledge?* (pp. 264-280). London, UK: Routledge.

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

Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*, 353-363. doi:10.1016/j.dss.2011.09.002

Law, J. (1986). On power and its tactics: A view from the sociology of science. *The Sociological Review*, *34*, 1-38. doi:10.1111/j.1467-954X.1986.tb02693.x

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice, 5*, 179-193. doi:10.1007/BF01059830

Lee, H., Harindranath, G., Oh, S., & Kim, D. (2015). Provision of mobile banking services from an actor–network perspective: Implications for convergence and standardization. *Technological Forecasting & Social Change, 90*, 551-561. doi:10.1016/j.techfore.2014.02.007

Lee, S., Oh, C. H., & Lee, J. Y. (2017). The effect of host country internet infrastructure on foreign expansion of Korean MNCs. *Asia Pacific Business Review*, 23, 396-419. doi:10.1080/13602381.2016.1156295

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY: Pearson.

Leins, D. A., Fisher, R. P., Pludwinski, L., Rivard, J., & Robertson, B. (2014). Interview protocols to facilitate human intelligence sources' recollections of meetings. *Applied Cognitive Psychology, 28*, 926-935. doi:10.1002/acp.3041

Lemieux, M. (2015). Cybercrime, governance, and liabilities in the banking and payment industries. *Banking & Finance Law Review, 31*, 113-140. Retrieved from https://www.bu.edu/rbfl/

Leng, S., MacDougall, M., & McKinstry, B. (2016). The acceptability to patients of video-consulting in general practice: Semi-structured interviews in three diverse general practices. *Journal of Innovation in Health Informatics, 23*, 493-500. doi:10.14236/jhi.v23i2.141

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

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. doi:10.1016/j.ijinfomgt.2018.10.017

Linton, J. (2017). *Strategies to support survivors of corporate downsizing* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10640881)

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*, 433-463. doi:10.1111/isj.12043

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

Lucas, M. L. (2018). *Exploring the strategies cybersecurity managers recommend for implementing or transitioning to the cloud* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10843999)

Lukka, K., & Vinnari, E. (2017). Combining actor-network theory with interventionist research: present state and future potential. *Accounting, Auditing & Accountability Journal, 30*, 720-753. doi:10.1108/AAAJ-08-2015-2176

Luppicini, R. (2014). Illuminating the dark side of the internet with actor-network theory: An integrative review of current cybercrime research. *Global Media Journal: Canadian Edition, 7*, 35-49. Retrieved from http://www.gmj.uottawa.ca/

Luscombe, A., & Walby, K. (2017). Theorizing freedom of information: The live archive, obfuscation, and actor-network theory. *Government Information Quarterly, 34*, 379-387. doi:10.1016/j.giq.2017.09.003

Maahs, D. L. (2018). *Managerial strategies small businesses use to prevent cybercrime* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10936342)

Malik, P., & Pretorius, L. (2018). A case study validation of the application of a generalized equation of innovation in complex adaptive systems. *South African Journal of Industrial Engineering, 20*, 1-20. doi:10.7166/29-1-1780

Mansfield-Devine, S. (2016). Securing small and medium-size businesses. *Network Security, 2016*, 14-20. doi:10.1016/S1353-4858(16)30070-8

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the target data breach. *Business Horizons, 59*, 257-266. doi:10.1016/j.bushor.2016.01.002

Marjanovic, O., & Cecez-Kecmanovic, D. (2017). Exploring the tension between transparency and datification effects of open government IS through the lens of

complex adaptive systems. *Journal of Strategic Information Systems, 26,* 210-232. doi:10.1016/j.jsis.2017.07.001

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Matua, G. A. (2015). Choosing phenomenology as a guiding philosophy for nursing research. *Nurse Researcher, 22*(4), 30-34. doi:10.7748/nr.22.4.30.e1325

Mawudor, B. G., Kim, M. H., & Park, M. G. (2015). Continuous monitoring methods as a mechanism for detection and mitigation of growing threats in banking security system. *2015 4th International Conference on Interactive Digital Media (ICIDM)*. doi:10.1109/idm.2015.7516317

Mbelli, T. M., & Dwolatzky, B. (2016). Cyber security, a threat to cyberbanking in South Africa: An approach to network and application security. *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*. doi:10.1109/cscloud.2016.18

McConnell-Henry, T., Chapman, Y., & Francis, K. (2011). Member checking and Heideggerian phenomenology: A redundant component. *Nurse Researcher, 18,* 28-37. doi:10.7748/nr2011.01.18.2.28.c8282

McCormack, M., Adams, A., & Anderson, E. (2013). Taking to the streets: The benefits of spontaneous methodological innovation in participant recruitment. *Qualitative Research, 13,* 228-241. doi:10.1177/1468794112451038

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative, or mixed methods and choice based on the research. *Perfusion*, *30*, 537-542. doi:10.1177/0267659114559116

McDermid, F., Peters, K., Jackson, D., & Daly, J. (2014). Conducting qualitative research in the context of pre-existing peer and collegial relationships. *Nurse Researcher, 21*, 28-33. doi:10.7748/nr.21.5.28.e1232

McGarry, O. (2016). Knowing 'how to go on': Structuration theory as an analytical prism in studies of intercultural engagement. *Journal of Ethnic & Migration Studies, 42*, 2067-2085. doi:10.1080/1369183X.2016.1148593

McKim, C. A. (2015). The value of mixed methods research: A mixed methods study. *Journal of Mixed Methods Research*, *20*, 202-222. doi:10.1177/1558689815607096

Mendez, J. V., Castillo, M. P. L., Sanchez, J. R., Mateus, J. D., & Maldonado, J. C. (2014). A software development for establishing optimal production lots and its application in academic and business environments. *Engineering and Research*, *34*, 81-86. doi:10.15446/ing.investig.v34n3.41578

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation*. San Francisco, CA: John Wiley & Sons.

Meszaros, J., & Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security*, *65*, 300-313. doi:10.1016/j.cose.2016.12.008

Michael, T., & Tiko, I. (2015). Politicking information technology strategy in organizations: A case study of a selected organization in South Africa. *Journal of Governance and Regulation*, *4*, 107-114. doi:10.22495/jgr_v4_i3_c1_p2

Modell, S., Vinnari, E., & Lukka, K. (2017). On the virtues and vices of combining theories: The case of institutional and actor-network theories in accounting research. *Accounting, Organizations and Society*, *60*, 62-78. doi:10.1016/j.aos.2017.06.005

Mohammed, D. (2015). Cybersecurity compliance in the financial sector. *Journal of Internet Banking and Commerce*, *20*(1), 1-11. Retrieved from http://www.arraydev.com/commerce/jibc/

Montenegro, L. M., & Bulgacov, S. (2015). Governance and strategy of undergraduate business programs in light of the actor-network theory. *Contemporary Administrative Magazine*, *19*, 212-231. Retrieved from http://www.scielo.br

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*, 1212-1222. doi:10.1177/1049732315588501

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

Mrabet, Z. E., Kaabouch, N., Ghazi, H. E., & Ghazi, H. E. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469-482. doi:10.1016/j.compeleceng.2018.01.015

Müller, M., & Schurr, C. (2016). Assemblage thinking and actor-network theory: Conjunctions, disjunctions, cross-fertilisations. *Transactions of the Institute of British Geographers*, *41*, 217-229. doi:10.1111/tran.12117

Namukasa, J. (2013). The influence of airline service quality on passenger satisfaction and loyalty. *TQM Journal, 25*, 520-532. doi:10.1108/tqm-11-2012-0092

Nasution, M. F., Dhillon, G., & Akyuwen, R. (2017). Shaping of security policy in an Indonesian bank: Interpreting institutionalization and structuration. *Kinerja*, *19*(1), 1-13. doi:10.24002/kinerja.v19i1.530

Nastasiu, C. (2016). Cybersecurity strategies in the Internet era. *Proceedings of the Scientific Conference AFASES, 2*, 619-624. doi:10.19062/2247-3173.2016.18.2.19

U.S. Department of Health and Human Services, National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the Protection of human subjects of research*. Retrieved from hhs.gov/ohrp/humansubjects/guidance/Belmont.html

Neghina, D., & Scarlat, E. (2013). Managing information technology security in the context of cyber-crime trends. *International Journal of Computers, Communications & Control, 8*, 97-104. Retrieved from http://journal.univagora.ro

Netkachova, K., & Bloomfield, R. E. (2016). Security-informed safety. *Computer, 49*, 98-102. doi:10.1109/MC.2016.158

Nevmerzhitskaya, J., Norvanto, E., & Virag, C. (2019). High impact cybersecurity capacity building. *E-Learning & Software for Education*, *2*, 306-312. doi:10.12753/2066-026X-19-113

Newington, L., & Metcalfe, A. (2014). Factors influencing recruitment to research: Qualitative study of the experiences and perceptions of research teams. *BMC Medical Research Methodology*, *14*, 1-20. doi:10.1186/1471-2288-14-10

Niedbalski, J., & Ślęzak. (2016). Computer analysis of qualitative data in literature and research performed by polish sociologists. *Forum: Qualitative Social Research*, *17*(3), 1-22. doi:10.17169/fqs-17.3.2477

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica*, *9*(3), 71-88. doi:10.2478/hjbpa-2018-0024

Northrup, J. C., & Shumway, S. (2014). Gamer widow: A phenomenological study of spouses of online video game addicts. *American Journal of Family Therapy*, *42*, 269-281. doi:10.1080/01926187.2013.847705

Ocasio, W., & Radoynovska, N. (2016). Strategy and commitments to institutional logics: Organizational heterogeneity in business models and governance. *Strategic Organizations*, *14*, 287-309. doi:10.1177/1476127015625040

Ogden, J., & Cornwell, D. (2010). The role of topic, interviewee, and question in predicting rich interview data in the field of health research. *Sociology of Health & Illness*, *32*, 1059-1071. doi:10.111/j.1467-9566.2010.01272.x

Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretations of verbal and nonverbal data in qualitative research. *International Journal of Education*, *6*, 183-246. doi:10.5296/ije.v6i1.43

Orser, B. J., Elliott, C., & Leck, J. (2011). Feminist attributes and entrepreneurial identity. *Gender in Management: An International Journal*, *26*, 561-589. doi:10.1108/17542411111183884

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health*, *42*, 533-544. doi:10.1007/s10488-013-0528-y

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*, *59*(3), 211-217. doi:10.1080/08874417.2019.1571459

Park, S., Kim, I. H., Kim, J., & Lee, K. L. (2018). The diagnosis and prescription for cybersecurity in Korea: Focusing on policy and system. *KSII Transactions on Internet and Information Systems*, *12*, 843-859. doi:10.3837/tiis.2018.02.018

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

Parker, E. (2017). An actor-network theory reading of change for children in public care. *British Educational Research Journal*, *43*, 151-167. doi:10.1002/berj.3257

Patel, M. R., Shah, K. S., & Shallcross, M. L. (2015). A qualitative study of physician perspectives of cost-related communication and patients' financial burden with managing chronic disease. *BMC Health Services Research, 15,* 151-157. doi:10.1186/s12913-015-1189-1

Patrascu, P. P. (2018). The appearance and development of national cybersecurity strategies. *Elearning & Software for Education, 4,* 453-59. doi:10.12753/2066-026X-18-222

Patterson, J. (2017). *Cyber-security policy decisions in small businesses* (Doctoral Dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10680962)

Patton, M. (2002). *Qualitative research and evaluation methods*. London, England: Sage.

Paulsen, C. (2016). Cybersecurity small businesses. *Computer (00189162), 49,* 92-97. doi:10.1109/MC.2016.223

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research. *Nurse Researcher, 22*(4), 6-7. doi:10.7748/nr.22.4.6.s2

Pieters, W. (2011). Explanation and trust: What to tell the user in security and AI? *Ethics & Information Technology, 13*(1), 53-64. doi:10.1007/s10676-010-9253-3

Pistol, L., & Rocsana, T. (2014). Models of marketing simulations for SMEs in Romania: Strategic game for marketing mix simulation. *Contemporary Readings in Law & Social Justice, 6,* 501-509. Retrieved from http://www.addletonacademicpublishers.com/

Pinfield, S., Cox, A. M., & Smith, J. (2014). Research data management and libraries: Relationships, activities, drivers, and influences. *Plos ONE, 9*, 1-28. doi:10.1371/journal.pone.0114734

Popescu, G. N., & Popescu, C. R. G. (2018). Risks of cyberattacks on financial audit activity. *Audit Financiar, 16*, 140-147.doi:10.20869/AUDITF/2018/149/140

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

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

Qu, S., & Dumay, J. (2011). The qualitative research interviews. *Qualitative Research in Accounting & Management*, *8*, 238-264. doi:10.1108/11766091111162070

Ramos-Villagrasa, P. J., Marques-Quinteiro, P., Navarro, J., & Rico, R. (2017). Teams as complex adaptive systems: Reviewing 17 years of research. *Small Group Research*, 49(2), 135-176. doi:10.1177/1046496417713849

Ravitch, S. M., & Carl, N. M. (2016). *Qualitative research: Bridging the conceptual, theoretical, and methodological*. Thousand Oaks, CA: Sage Publications.

Reid, M. L. (2016). *Adoption of electronic health record systems within primary care practices* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 1781660022)

Reid, R., & Van Niekerk, J. (2014). 2014 *Information Security for South Africa, Information Security for South Africa (ISSA), 2014*, 1. doi:10.1109/ISSA.2014.6950492

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

Reiter, S., Stewart, G., & Bruce, C. (2011). A strategy for delayed research method selection: Deciding between grounded theory and phenomenology. *The Electronic Journal of Business Research Methods, 9,* 35-46. Retrieved from http://www.ejbrm.com/

Resnik, D. B., Miller, A. K., Kwok, R. K., Engel, L. S., & Sandler, D. P. (2015). Ethical issues in environmental health research related to public health emergencies: Reflections on the Gulf study. *Environmental Health Perspectives, 123,* A227–A231. doi:10.1289/ehp.1509889

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

Rocci, L. (2014). Illuminating the dark side of the internet with actor-network theory: An integrative review of current cybercrime research. *Global Media Journal: Canadian Edition, 7,* 35-49. Retrieved from http://www.gmj.uottawa.ca/

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

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

Ryan, G. S. (2013). Online social networks for patient involvement and recruitment in clinical research. *Nurse Researcher*, *21*, 35–39. doi:10.7748/nr2013.09.21.1.35.e302

Rydwik, E. E., Bergland, A. A., Forsén, L. L., & Frändin, K. K. (2012). Investigation into the reliability and validity of the measurement of elderly people's clinical walking speed: A systematic review. *Physiotherapy Theory & Practice*, *28*, 238-256. doi:10.3109/09593985.2011.601804

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

Saber, A. (2016). *Determining small business cybersecurity strategies to prevent data breaches* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 1834016856)

Sadoway, D., & Gopakumar, G. (2017). (Un)bundling Bangalore: Infrastructure bundling 'best practices' and assembling novel scapes. *Geoforum, 79*, 7946-7957. doi:10.1016/j.geoforum.2016.12.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organizations.

Journal of Information Security and Applications, *40*, 247-257. doi:10.1016/j.jisa.2017.11.001

Samnani, A., & Singh, P. (2013). Exploring the fit perspective: An ethnographic approach. *Human Resource Management, 52,* 123-144. doi:10.1002/hrm.21516

Sargeant, J. (2012). Qualitative research part II: Participants, analysis, and quality assurance. *Journal of Graduate Medical Education, 4*(1), 1-3. doi:10.4300/JGME-D-11-00307.1

Sayes, E. (2017). Marx and the critique of actor-network theory: Mediation, translation, and explanation. *Distinktion: Journal of Social Theory, 18*, 294-313. doi:10.1080/1600910X.2017.1390481

Scully, T. (2013). The cybersecurity threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning*, *7*(2), 138–148. Retrieved from http://www.henrystewartpublications.com/

Selznick, L. F., & Lamacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law*, *13*, 217-253. Retrieved from http://www.law.umaryland.edu/journal/jbtl/

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

Senol, M. (2017). An approach for creation and implementation of national cybersecurity strategy. *2017 International Conference on Computer Science and Engineering (UBMK)*. doi:10.1109/ubmk.2017.8093373

Sepulveda, D. A. (2017). The role of leadership in internet governance. *Fletcher Forum of World Affairs, 41,* 129-139. Retrieved from http://www.fletcherforum.org/

Sergeeva, A., Huysman, M., Soekijad, M., & van den Hooff, B. (2017). Through the eyes of others: How onlookers shape the use of technology at work. *MIS Quarterly, 41,* 1153-1178. doi:10.25300/misq/2017/41.4.07

Servidio, J. S., & Taylor, R. D. (2015). Safe and sound: Cybersecurity for community banks. *Journal of Taxation & Regulation of Financial Institutions, 28,* 5-14. Retrieved from http://www.civicresearchinstitute.com

Shahin, A., Jamkhaneh, B. H., & Cheryani, Z. H. S. (2014). EFQMQual: Evaluating the implementation of the European quality award based on the concepts of model of service quality gaps and ServQual approach. *Measuring Business Excellence, 18,* 56-38. doi:10.1108/MBE-12-2012-0057

Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications, 36*(2017), 1-10. doi:10.1016/j.jisa.2017.07.004

Shan, L. C., Panagiotopoulos, P., Regan, Á., De Brún, A., Barnett, J., Wall, P., & McConnon, Á. (2015). Interactive communication with the public: Qualitative exploration of the use of social media by food and health organizations. *Journal of Nutrition Education and Behavior, 47,* 104-108. doi:10.1016/j.jneb.2014.09.004

Sheedy, E. A., Griffin, B., & Barbour, J. P. (2017). A framework and measure for examining risk climate in financial institutions. *Journal of Business and Psychology, 32,* 101-116. doi:10.1007/s10869-015-9424-7

Shim, Y., & Shin, D. (2016). Analyzing China's fintech industry from the perspective of actor–network theory. *Telecommunications Policy, 40,* 168-181. doi:10.1016/j.telpol.2015.11.005

Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. *Politics & Governance, 6,* 31-40. doi:10.17645/pag.v6i2.1329

Sipes, E. K., James, J., & Zetoony, D. (2016). Current data security issues for financial services firms. *Journal of Investment Compliance (Emerald Group), 17,* 55-59. doi:10.1108/JOIC-07-2016-0034

Schneider, F. B. (2018). Impediments with policy interventions to foster cybersecurity. *Communications of the ACM, 61,* 36-38. doi:10.1145/3180493

Scrutton, R., & Beames, S. (2015). Measuring the unmeasurable: Upholding rigor in quantitative studies of personal and social development in outdoor adventure education. *Journal of Experiential Education, 38,* 8-25. doi:10.1177/1053825913514730

Shields, P., & Rangarjan, N. (2013). *A playbook for research methods: Integrating conceptual frameworks and project management*. Stillwater, OK: New Forums Press.

Siddiqui, N., & Fitzgerald, J. A. (2014). Elaborated integration of qualitative and quantitative perspectives in mixed methods research: A profound enquiry into the

nursing practice environment. *International Journal of Multiple Research Approaches, 8,* 137-147. doi:10.5172/mra.2014.8.2.137

Singh, K. D. (2015). Creating your own qualitative research approach: Selecting, integrating, and operationalizing philosophy, methodology, and methods. *Vision, 19,* 132-146. doi:10.1177/0972262915575657

Singh, A. N., & Gupta, M. P. (2019). Information security management practices: Case studies from India. *Global Business Review, 20,* 253-271. doi:10.1177/0972150917721836

Small, W., Maher, L., & Kerr, T. (2014). Institutional ethical review and ethnographic research involving injection drug users: A case study. *Social Science & Medicine, 104,* 157-162. doi:10.1016/j.socscimed.2013.12.010

Smith, J. A., Wilde, M. H., & Brasch, J. (2012). Internet recruitment and retention for a six months' longitudinal study. *Journal of Nursing Scholarship, 44,* 165-170. doi:10.1111/j.1547-5069.2012.01446.x

Soltanizadeh, S., Abdul Rasid, S. Z., Mottaghi Golshan, N., & Wan Ismail, W. K. (2016). Business strategy, enterprise risk management, and organizational performance. *Management Research Review, 39,* 1016-1033. doi:10.1108/MRR-05-2015-0107

Stack, R. J., Sahni, M., Mallen, C. D., & Raza, K. (2013). Symptom complexes at the earliest phases of rheumatoid arthritis: A synthesis of the qualitative literature. *Arthritis & Rheumatism, 65,* 1916-1926. doi:10.1002/acr.22097

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

Stechyshyn, A. (2015). *Security vulnerabilities in financial institutions* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 1677223944)

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

Srinivasan, B. N., & Mukherjee, D. (2018). Agile teams as complex adaptive systems (CAS). *International Journal of Information Technology, 10*, 367-378. doi:10.1007/s41870-018-0122-3

Sweeney, M., & Goldblatt, J. (2016). An exploration of mixed research methods in planned event studies. *Journal of Convention & Event Tourism, 17*, 41-54. doi:10.1080/15470148.2015.1084602

Svensson, L., & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative Inquiry, 19*, 441-450. doi:10.1177/1077800413482097

Sunday, C., & Vera Chinwedu, C. (2018). Strategic roles of actors in emerging information communication technology (EICT) adoption in SMEs : Actor-network theory analysis. *The Bottom Line, 31*, 114-136. doi:10.1108/BL-09-2017-0029

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal, 11*, 63-75. doi:10.3316/QRJ1102063

Tabassum, A., Mustafa, M. S., & Maadeed, S. A. A. (2018). The need for a global response against cybercrime: Qatar as a case study. *2018 6th International Symposium on Digital Forensic and Security (ISDFS), Digital Forensic and Security (ISDFS), 2018 6th International Symposium on*, 1. doi:10.1109/ISDFS.2018.8355331

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

Teusner, A. (2015). Insider research, validity issues, and the OHS professional: *One International Journal of Social Research Methodology, 19*(1), 85-96. doi:10.1080/13645579.2015.1019263

Titze, K., Schenck, S., Logoz, M., & Lehmkuhl, U. (2014). Assessing the quality of the parent-child relationship: Validity and reliability of the child-parent relationship test (ChiP-C). *Journal of Child & Family Studies, 23*, 917-933. doi:10.1007/s10826-013-9749-7

Thomas, G. (2013). *How to do your research project*. Thousand Oaks, CA: Sage Publications.

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

Trainor, A., & Bouchard, K. A. (2013). Exploring and developing reciprocity in research design. *International Journal of Qualitative Studies in Education*, *26*, 986-1003. doi:10.1080/09518398.2012.724467

Treharne, G. J., & Riggs, D. W. (2015). Ensuring quality in qualitative research. *Qualitative Research in Clinical and Health Psychology*, 57-73. doi:10.1007/978-1-137-29105-9_5

Trim, P. R. J., & Lee, Y. I. (2010). A security framework for protecting business, government, and society from cyber attacks. *2010 5th International Conference on System of Systems Engineering*. doi:10.1109/sysose.2010.5544085

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organizations. *European Journal of Information Systems*, *24*, 38-58. Retrieved from https://www.palgrave.com/us/journal/41303

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

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

Ülle, P. (2014). The role of dialogue between executives and ground-level employees mediated by MACS. *Baltic Journal of Management, 9,* 189-212. doi:10.1108/BJM-10-2013-0153

Unkovic, C., Sen, M., & Quinn, K. M. (2016). Does encouragement matter in improving gender imbalances in technical fields? Evidence from a randomized controlled trial. *PLoS One, 11*(4), 1-32. doi:10.1371/journal.pone.0151714

Valipoor, S., & Pati, D. (2016). Making your instruments work for you. *HERD: Health Environments Research & Design Journal, 9,* 236-243. doi:10.1177/1937586715601423

Van Brussel, S., Boelens, L., & Lauwers, D. (2016). Unraveling the Flemish mobility orgware: The transition towards a sustainable mobility from an actor-network perspective. *European Planning Studies*, *24*, 1336-1356. doi:10.1080/09654313.2016.1169248

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology, 55*, 578-595. doi:10.1093/bjc/azv009

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

Wagner, W., Hansen, K., & Kronberger, N. (2014). Quantitative and qualitative research across cultures and languages: Cultural metrics and their application. *Integrative Psychological & Behavioral Science*, *48,* 418-434. doi:10.1007/s12124-014-9269-z

Wairokpam, P. D., & Kumar, H. (2018). Frugal innovations and actor–network theory: A case of bamboo shoots processing in Manipur, India. *The European Journal of Development Research*, *30*(1), 66-83. doi:10.1057/s41287-017-0116-1

Wall, S. (2015). Focused ethnography: A methodological adaptation for social research in emerging contexts. *Forum: Qualitative Social Research, 16*(1), 1-15. doi:10.17169/fqs-16.1.2182

Walters, I. (2017). *Strategies for recruiting cybersecurity professionals in the financial service industry* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10606902)

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

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers perceptions. *International Journal of the Academic Business World*, *12*, 23-30. Retrieved from http://jwpress.com/

Weaver, S. T., Ellen, P. S., & Mathiassen, L. (2015). Contextualist inquiry into organizational citizenship: Promoting recycling across heterogeneous organizational actors. *Journal of Business Ethics*, *129*, 13-28. doi:10.1007/s10551-014-2165-0

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*(2014), 1-15. doi:10.1016/j.cose.2014.04.005

Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based leadership development: Insights from expert coaches. *Consulting Psychology Journal: Practice & Research, 66*, 20-37. doi:10.1037/cpb0000002

Weldearegay, T. (2017). *E-business strategy to adopt electronic banking services in Ethiopia* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 10639443)

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43-57. doi:10.1016/j.ijinfomgt.2003.12.003;

Wilgus, M. (2018). The dangers in perpetuating a culture of risk acceptance. *Information System Security Association Journal*, *16*(4), 20-43. Retrieved from https://www.issa.org/

Williams, C. (2014). Security in the cyber supply chain: Is it achievable in a complex, interconnected world? *Technovation*, *34*, 382-384. doi:10.1016/j.technovation.2014.02.003

Wilson, A. (2015). A guide to phenomenological research. *Nursing Standard, 29*(34), 38-43. doi:10.7748/ns.29.34.38.e8821

Wisdom, J. P., Cavaleri, M. A., Onwuegbuzie, A. J., & Green, C. A. (2012). Methodological reporting in qualitative, quantitative, and mixed methods health services research articles. *Health Services Research*, *47*, 721-745. doi:10.1111/j.1475-6773.2011.01344.x

Wray, J., Archibong, U., & Walton, S. (2017). Why undertake a pilot in a qualitative Ph.D. study? Lessons learned to promote success. *Nurse Researcher*, *24*, 31-35. doi:10.7748/nr.2017.e1416

Yang, S. O., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling effective operational risk management in a financial institution: An action research study. *Journal of Management Information Systems*, *34*, 727-753. doi:10.1080/07421222.2017.1373006

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *Qualitative Report*, *20*, 134-152. Retrieved from http://www.nova.edu/tqr/

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

Young, D., Borland, R., & Coghill, K. (2012). Changing the tobacco use management system: Blending systems thinking with actor-network theory. *Review of Policy Research*, *29*, 251-279. doi:10.1111/j.1541-1338.2011.00550.x

Zawawi, N. H. M. (2018). Actor-network theory and inter-organizational management control. *International Journal of Business & Society*, *19*, 219-234. Retrieved from http://www.ijbs.unimas.my/

Appendix: Interview Protocol

Date of Interview: _____ Code Assigned: _____

1. Introduce self to participant(s).
2. Introduce the research topic.
3. Thank the participant for taking the time to respond to the invitation to participate in the study
4. The present consent form goes over the contents and answers questions and concerns of the participant.
5. Give participant copy of consent form for review.
6. Turn on the recording device.
7. Follow the procedure to introduce the participant(s) with pseudonym/coded identification; note the date and time.
8. Begin the interview with question #1. The meeting will span 30-45 minutes for responses to the interview questions, including any additional follow-up questions.
9. Remind the participant of the purpose of the proposal is to explore the strategies some leaders of small financial institution use to protect information systems from cyber threats.
10. End interview sequence; discuss the follow-up member checking process with each participant.
11. Thank the participant(s) for their part in the study. Reiterate contact numbers for follow-up questions and concerns from participants.