

2019

# Strategies for Improving Data Protection to Reduce Data Loss from Cyberattacks

Jennifer Elizabeth Cannon  
*Walden University*

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

 Part of the [Business Commons](#)

---

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact [ScholarWorks@waldenu.edu](mailto:ScholarWorks@waldenu.edu).

# Walden University

College of Management and Technology

This is to certify that the doctoral study by

Jennifer E. Cannon

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. Peter Anthony, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Jaime Klein, Committee Member, Doctor of Business Administration Faculty

Dr. Matthew Knight, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer  
Eric Riedel, Ph.D.

Walden University  
2019

Abstract

Strategies for Improving Data Protection to Reduce Data Loss from Cyberattacks

by

Jennifer E. Cannon

MS, Troy University, 2006

BS, University of South Florida, 2000

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2019

## Abstract

Accidental and targeted data breaches threaten sustainable business practices and personal privacy, exposing all types of businesses to increased data loss and financial impacts. This single case study was conducted in a medium-sized enterprise located in Brevard County, Florida, to explore the successful data protection strategies employed by the information system and information technology business leaders. Actor–network theory was the conceptual framework for the study with a graphical syntax to model data protection strategies. Data were collected from semistructured interviews of 3 business leaders, archival documents, and field notes. Data were analyzed using thematic, analytic, and software analysis, and methodological triangulation. Three themes materialized from the data analyses: people--inferring security personnel, network engineers, system engineers, and qualified personnel to know how to monitor data; processes--inferring the activities required to protect data from data loss; and technology--inferring scientific knowledge used by people to protect data from data loss. The findings are indicative of successful application of data protection strategies and may be modeled to assess vulnerabilities from technical and nontechnical threats impacting risk and loss of sensitive data. The implications of this study for positive social change include the potential to alter attitudes toward data protection, creating a better environment for people to live and work; reduce recovery costs resulting from Internet crimes, improving social well-being; and enhance methods for the protection of sensitive, proprietary, and personally identifiable information, which advances the privacy rights for society.

Strategies for Improving Data Protection to Reduce Data Loss from Cyberattacks

by

Jennifer E. Cannon

MS, Troy University, 2006

BS, University of South Florida, 2000

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2019

## Dedication

Some people walk into your life and make little impact on your path. Others walk into your life, make a profound impression, and leave an everlasting mark on your soul. I dedicate this work of heart to one such person, the love of my life, my best friend, and confidant. I also dedicate this work to our children, all of whom sacrificed their time and 4 years of their lives to support me in this endeavor. I further dedicate this work to my parents who provided support, encouragement, and most importantly their genetic material, and that of my ancestors, coding my motivations and desires to achieve great things in life. An additional dedication to my sister, her husband, and my nieces and nephew, all of whom provided humor and gracious smiles when I needed them most.

A final dedication to the men and women, quietly and sometimes without recognition, battling the cyberspace war on a day-to-day basis to protect our nation's data.

*Data are the building blocks of information unlocking our potential as a species in defining our interpretations, philosophies, and perceptions of the world, societies, and individuals. Humans can innovate monumental wonders if we can only protect the information that arises from our data. ~Jennifer E. Cannon*

## Acknowledgments

First and foremost, I recognize the mentorship, guidance, and friendship offered by Dr. Peter Anthony. There were times through this process the struggles felt insurmountable, and Dr. Anthony gave perspective to the situation. His facilitation of the DBA process, availability, and his above and beyond attitude made a lasting impression. Thank you.

My sincerest appreciation to Dr. Jaime Klein and Dr. Matthew Knight for their continued patience and professionalism with my study. Your combined insights and feedback elevated my opus to a quality product. Thank you.

I extend my deepest appreciation to the partnering organization and the participants that volunteered their time and input to this study. Thank you.

I would also like to acknowledge the countless hours my husband and oldest daughter provided editing, providing feedback, and reviewing my work. Thank you.

To all the people who contributed in small and large ways to make this dream a reality. These are my colleagues at DHS, DSS, Walden University, my life-long friends, my newer friends, my peeps from Florida and Denver, and the experts whom I met along the way. Thank you.

## Table of Contents

List of Tables .....	v
List of Figures .....	vi
Section 1: Foundation of the Study.....	1
Background of the Problem .....	1
Problem Statement.....	2
Purpose Statement.....	3
Nature of the Study .....	3
Research Question .....	4
Interview Questions .....	5
Conceptual Framework.....	6
Operational Definitions.....	6
Assumptions, Limitations, and Delimitations.....	8
Assumptions.....	8
Limitations .....	9
Delimitations.....	9
Significance of the Study .....	10
Contribution to Business Practice.....	10
Implications for Social Change.....	11
A Review of the Professional and Academic Literature.....	11
Actor-Network Theory (ANT).....	13
Data Regulation .....	19



Data Threats .....	22
Data Risk.....	30
Data Breaches .....	31
Data Loss Prevention .....	34
Data Security Breach Notification and Recovery.....	35
Data Protection.....	37
Alternative Theories.....	41
Transition .....	43
Section 2: The Project.....	45
Purpose Statement.....	45
Role of the Researcher .....	46
Participants.....	49
Research Method and Design .....	52
Research Method .....	52
Research Design.....	55
Population and Sampling .....	59
Defining a Population .....	59
Sampling .....	60
Ethical Research.....	62
Data Collection Instruments .....	66
Data Collection Technique .....	68
Data Organization Technique .....	71

Data Analysis .....	72
Reliability and Validity.....	74
Reliability.....	74
Validity .....	76
Transition and Summary.....	76
Section 3: Application to Professional Practice and Implications for Change .....	78
Introduction.....	78
Presentation of the Findings.....	79
Member-Checked Interviews Themes .....	81
Researcher Field Notes Themes.....	83
Archival Documents Themes.....	86
Methodological Triangulation of Coded Themes .....	88
ANT-gs, Data Protection Strategy, and Reducing Data Loss.....	97
Summary of the Findings.....	107
Applications to Professional Practice .....	108
Implications for Social Change.....	111
Recommendations for Action .....	112
Recommendations for Further Research.....	113
Reflections .....	116
Conclusion .....	117
References.....	119
Appendix A: Interview Protocol.....	150

Appendix B: Member Checking Letter.....	153
Appendix C: Observation Protocol.....	154
Appendix D: Journaling Protocol .....	155

## List of Tables

Table 1 <i>Frequency of Member-Checked Interview Themes</i> .....	81
Table 2 <i>Frequency of Researcher Field Notes Themes</i> .....	84
Table 3 <i>Frequency of Archival Documents Themes</i> .....	87
Table 4 <i>Frequency of Triangulated Themes</i> .....	89
Table 5 <i>Meanings of ANT-gs Symbols</i> .....	99

## List of Figures

<i>Figure 1.</i> Data protection strategies mind map of themes from literature review.....	79
<i>Figure 2.</i> Word frequency query results for member-checked interviews. ....	83
<i>Figure 3.</i> Word frequency query results for researcher field notes. ....	86
<i>Figure 4.</i> Word frequency query results for archival documents. ....	88
<i>Figure 5.</i> Word frequency query results for triangulated data.....	90
<i>Figure 6.</i> Encounter-episode framework for architecture security strategy .....	102
<i>Figure 7.</i> Encounter-episode 1 of architecture security strategy. ....	104
<i>Figure 8.</i> Encounter-episode 2 of architecture security strategy. ....	104
<i>Figure 9.</i> Encounter-episode 3 of architecture security strategy. ....	105
<i>Figure 10.</i> Encounter-episode 4 of architecture security strategy. ....	105
<i>Figure 11.</i> Encounter-episode 5 of architecture security strategy. ....	106
<i>Figure 12.</i> Encounter-episode 6 of architecture security strategy. ....	106
<i>Figure 13.</i> Encounter-episode 7 of architecture security strategy. ....	107

## Section 1: Foundation of the Study

Data loss continues to present challenges to organizations, which are increasing with technological advances and information exchange. Business leaders, information technology (IT) and information system (IS) professionals, and individuals need strategies to protect data at work, home, or while traveling. Data security is no longer an IT function of creating a perimeter around the system containing the sensitive data. Instead, IT practitioners are developing data protection strategies surrounding data elements. Data security is digital security to secure information systems, enabling the development and transmission of data electronically. Data security is a combination of data protection methods for a variety of sociotechnological environments.

### **Background of the Problem**

Data loss is responsible for many businesses experiencing loss of reputation, revenue, customer loyalty, and competitive advantage (Malecki, 2014). The common denominators in data loss are humans, weak cybersecurity (Gayomali, 2014), and a false sense of security in technology. Some people cannot resist the urge to click links, some companies do not acknowledge the importance of investing in cybersecurity (Gayomali, 2014), and other companies implement technology as their only defense (Ernst & Young Global Limited, 2014). Victims of cybercrimes lost approximately 55 million dollars in 2015 (Federal Bureau of Investigation Internet Crime Complaint Center [FBI ICC], 2016). Within the same year, statistics show business managers suffering data breach damages totaling 11.9 billion dollars and economic impacts of 4.26 billion dollars (National Intellectual Property Rights Coordination Center, 2015).

Business leaders continue to experience concerns with data breaches and data loss. The National Cybersecurity and Communications Integration Center recorded numerous reports of cyberattacks that highlight a gap in data protection strategies used by business leaders (Claus, Gandhi, Rawnsley, & Crowe, 2015), which allow cyber attackers cause financial hardships for U.S. business leaders. These continued financial hardships result in business leaders increasing investment in data protection to mitigate remediation costs (The Ponemon Institute, 2016). Moreover, in 2018, business leaders faced new cost concerns with the enactment of the general data protection regulation (GDPR) in Europe (Ceross, 2018). Business leaders across the globe must now report how European citizens personal information is controlled or face immense fines (Ceross, 2018; Kennedy & Millard, 2016). Business leaders require a data protection solution to minimize financial hardship while enabling innovation and growth. Therefore, business leaders' lack of everyday data protection methods was a relevant business problem for research.

### **Problem Statement**

The Government Accountability Office (2015a) reported an increase in cyberattack attempts from 10,481 in 2009 to 27,624 in 2014 to access sensitive data. In 2014, the Pew Research Center reported 22.9% of medium-sized U.S. businesses experienced data breaches (Fitzpatrick & Dilullo, 2015). Victim losses reached \$1.33 billion in 2016 with corporate data breaches ranking in the top five victim loss categories (FBI ICCC, 2016). In 2017, the FBI ICCC annual report analysts reported a 5-year total of 1,420,555 complaints with financial losses of \$5.52 billion (FBI ICCC, 2017). The general business problem is that cyberattacks on businesses cause loss of data and a

negative financial impact. The specific business problem is that some medium-sized enterprise (ME) business leaders lack strategies to improve data protection to reduce data loss from cyberattacks.

### **Purpose Statement**

The purpose of this qualitative, single case study was to explore the strategies that ME business leaders use to improve data protection to reduce data loss from cyberattacks. The targeted population for this study included three ME business leaders from a global worldwide services company in Brevard County, Florida. These ME business leaders implemented strategies that improved data protection and reduced data loss from cyberattacks. Business leaders' acceptance of the study's findings might spread the use of effective strategies for reducing data losses and recovery costs. ME owners reducing data loss from cyberattacks can contribute to positive social change by altering attitudes toward data protection, reducing costs associated with protection against Internet crimes, and enhancing an individual's capabilities in the protection of sensitive, proprietary, and personally identifiable information (PII).

### **Nature of the Study**

I implemented a qualitative methodology for this study. Qualitative researchers develop a subjective view of a population's behavior associated with phenomena (Willan, 2016). As the purpose of this study was to explore the strategies that ME business leaders use to improve data protection to reduce data loss from cyberattacks, a qualitative method was appropriate. In contrast, quantitative researchers use data in support of a theory or hypothesis quantifying the rejection of the null hypothesis (Neal & Ilsever, 2016). I



developed an interpretation of data protection strategies versus quantifying the data protection strategies, which made the goals of a quantitative approach inappropriate for this study. Additionally, mixed methods are an advanced approach combining qualitative and quantitative research methods (Neal & Ilsever, 2016); however, I only needed a qualitative methodology, so a mixed-method approach was unsuitable for this study.

I used a single case study for this study. Researchers use a case study design to explain *why* and *how* (Väyrynen, Hekkala, & Liias, 2013). I used this design to explain why and how business leaders successfully implemented data protection strategies for reducing data losses from cyberattacks. Another potential design was ethnography, which is used for understanding and explaining a group of individuals' cultures (Baskerville & Myers, 2014); however, this design was not appropriate because I did not characterize the culture of ME business leaders. Additionally, because I explored data protection strategies ME business leaders used to reduce data loss, a phenomenological design was improper for this study. Finally, researchers using a narrative design gain an understanding of participants' stories through ordered events (Kruth, 2015), but I conducted a study of *why* and *how* ME business leaders implemented data protection strategies, making a narrative design unsuitable for the purpose of this study.

### **Research Question**

What strategies do ME business leaders use to improve data protection to reduce data loss from cyberattacks?

### Interview Questions

1. What strategies have you used to improve data protection to reduce data loss resulting from cyberattacks?
2. What strategies did you find worked best to improve data protection to reduce data loss resulting from cyberattacks?
3. What are some examples of technical threats to your firm's data that influenced your selection of strategies to improve data protection to reduce data loss resulting from cyberattacks?
4. What are some examples of nontechnical threats to your firm's data that influenced your selection of strategies to improve data protection to reduce data loss resulting from cyberattacks?
5. What, if any, types of training were offered or required for your personnel to contribute to the implementation of the selected strategies?
6. How did you determine your chosen strategies were successful in improving data protection and reducing data loss?
7. How did you address key challenges to implementing your chosen strategies to improve data protection to reduce data loss?
8. What additional information can you contribute that you have not previously addressed about improving data protection to reduce data loss resulting from cyberattacks?

## **Conceptual Framework**

To explore the strategies that ME business leaders use to improve data protection to reduce data loss from cyberattacks, I used the actor-network theory (ANT) as the conceptual framework. The ANT was developed as a collaboration between Michel Callon and John Law (1997) and Bruno Latour (1996). The theorists' fundamental concept is anchored on the translations between human (i.e., actors) and nonhuman (i.e., actants) entities through the sociology of science and technology (Jackson, 2015). The theorists suggest that heterogeneous entities, human and nonhuman, join in creation as a networked system and emerging as a singular entity (Latour, 2011). The fundamental proposition of the theory is the innovation of an idea that develops into a network through the interactions of actors and actants (Thumlert, de Castell, & Jenson, 2015; Walls, 2015). The ANT fit the purpose of my study by helping to identify ME business leaders (i.e., actors) and data protection strategies (i.e., actants) in a network of translations that spreads ideas to improve data protection and reduce data loss resulting from cyberattacks.

## **Operational Definitions**

The clarification of technical terms in this study is important to deliver understanding of data protection strategies ME business leaders use to improve data protection to reduce data loss from cyberattacks.

*Actors and actants:* Actors and actants are any material or substance (i.e., human or nonhuman) capable of interacting in a network of aligned interests that propagate an idea (Desai et al., 2017; Elder-Vass, 2015; Jackson, 2015).

*Advanced persistent threat:* Advanced persistent threat is the long-term attack on an IS orchestrated for an extended period against a business to harvest business critical information through continuous monitoring of the system by an attacker (Baskerville, Spagnoletti, & Kim, 2014; Kaukola, Ruohonen, Tuomisto, Hyrynsalmi, & Leppänen, 2017).

*Business-critical information (BCI):* BCI is the information considered proprietary, sensitive, or not, within an organization that is an asset requiring a protection strategy (Kaukola et al., 2017).

*C-I-A principle:* The C-I-A principle is the three dimensions of data protection involving the confidentiality, integrity, and availability of data through varying protections (Rahimian, Bajaj, & Bradley, 2016).

*Data loss prevention (DLP):* DLP is the detection of data in transit through system processes to prevent data loss (Arbel, 2015).

*Data leakage:* Data leakage is the inadvertent or malevolent loss of data through disclosure to unauthorized users (J.-S. Wu, Lin, Lee, & Chong, 2015).

*Data theft:* Data theft is the illegal access to a company's information associated with the company's customers (Hinz, Nofer, Schiereck, & Trillig, 2015).

*Information technology function:* Information technology function is the perspective of risk to an information security system as a compromise of IT security controls (Rahimian et al., 2016).

*Insider threat:* Insider threat is an individual's use of their authorized access to an organization's data to knowingly or unwittingly cause harm (Center for Development of Security Excellence, 2018).

*Security threat:* Security threat is the potential exploitation of weakness or vulnerability within an IS (Kaukola et al., 2017).

*Vulnerability:* Vulnerability is an attribute of a business asset that indicates the asset is vulnerable to threats (Hutchins et al., 2015).

### **Assumptions, Limitations, and Delimitations**

Researchers enhance the outcomes of a study by understanding the possible assumptions, limitations, and delimitations impacting the study (Simon & Goes, 2003). I understood the importance of acknowledging the study assumptions, limitations, and delimitations to enhance the outcomes. The following is a discussion of the assumptions, limitations, and delimitations relative to my study.

#### **Assumptions**

An assumption is the formation of beliefs that exist independently and without confirmation of the knowledge (Ma, 2015). I considered several facts true but unverified within my study. In qualitative research, an assumption is personal, subjective, unique, multilayered, and with many interpretations (Ma, 2015). I acknowledged six underlying assumptions in my study. First, I assumed that semistructured interviews and review of company documents would provide enough data to develop themes within data protection, provide an answer to and support the overarching question, and support triangulation. I also assumed that conducting face-to-face interviews with willing

participants would yield a relative and honest response. Another assumption I made was that the resulting data protection strategies from this study will provide business leaders a means to protect sensitive and proprietary data from loss. I further assumed the ANT is a viable framework for business leaders to comprehend the implementation of data protection strategies to reduce data loss. A final assumption was that use of the ANT framework would reduce personal bias sufficiently to demonstrate the usefulness of the framework in sociotechnical environments. My assertion of assumptions potentially mitigated bias and supports my objectivity.

### **Limitations**

Limitations are potential weaknesses or problems specific to the research question with impact on validity and transferability but outside the control of the researcher (Connelly, 2013; Ellis & Levy, 2009; Yilmaz, 2013). A limitation of this study was the participant's responses. As the interviewer, I provided semistructured questions, but the quality and honesty of the participants' responses relevant to the research question was out of my control. Another limitation was the time needed to support this study. A shortened study timeframe limited the amount of useful data gained. A final limitation with this study was the use of specific data collection instruments (i.e., interviews and archival documents). The use of semistructured interviews and review of documents may have limited the rich data available to support my research question.

### **Delimitations**

A delimitation bounds or scopes a research study (Willan, 2016). There are several delimitations to my study. The study is delimited to ME business leaders within a

global worldwide services company licensed in Brevard County, Florida. I delimited the sample size with five IS/IT managers from the population of ME business leaders available within the selected case study facility. The selected case study company demonstrated the successful application of data protection strategies against cyberattacks with zero data breaches within the last 3 years. I delimited the data collection to semistructured interviews and archival documents excluding other potential types of data collection that may provide relevance to this research. Another delimiter I implemented was the use of the ANT to frame my approach to understanding data protection strategies (Elder-Vass, 2015; Jackson, 2015). Other theories may offer frameworks for business leaders to comprehend and implement the findings of the study. Finally, I chose Brevard County, Florida as my geographical location due to the proximity of my home and my knowledge of the businesses in the area limiting other potential geographical areas.

### **Significance of the Study**

#### **Contribution to Business Practice**

The contributions to business practice involve improving data protection to reduce data losses and recovery costs for business leaders. ME business leaders capable of improving data loss reduce recovery costs and improve business performance (Hausken, 2014). The repercussions of businesses not protecting their data can include bankruptcy, loss of competitive advantage, and general financial distress (Srinidhi, Yan, & Tayi, 2015). However, the application of security-enhancement assets positively affects the financial disposition of a company (Srinidhi et al., 2015). ME business leaders implementing data protection strategies may improve business operations leading to

improved financial health and overall performance. Companies continue to experience cyberattacks as a threat to business data (Crowley & Johnstone, 2016), but ME business leaders proficient in reducing data loss from cyberattacks increase the positive external perceptions for their company (Martin, Borah, & Palmatier, 2017) and increase competitive advantage. These study findings may provide information to facilitate increased organizational performance through a reduction of recovery costs related to data security breaches.

### **Implications for Social Change**

Data protection is a requirement for public and private business operations. The digital exchange of information supports hundreds of billions of dollars in yearly transactions (Government Accountability Office, 2015b). Business and world leaders must strive for both privacy and security by developing improved data protection methods to work toward data protection solutions, which can benefit everyone (Hare, 2016). Based on the findings of this study, ME owners might contribute to positive social change by altering attitudes toward data protection, creating a better environment for people to live and work; reducing recovery costs from Internet crimes, improving social well-being; and enhancing methods for the protection of sensitive, proprietary, and PII advancing the privacy rights for society.

### **A Review of the Professional and Academic Literature**

The purpose of this qualitative, single case study was to explore the strategies that ME business leaders use to improve data protection to reduce data loss from cyberattacks. Previous studies have been focused on cybersecurity and the financial impacts from weak



cybersecurity (Cook, 2017; Kongnso, 2015). Business leaders impacted by the data loss and financial impacts potentially incur increased risks affecting business performance and competitive advantage (Cook, 2017; Crowley & Johnstone, 2016; Desai et al., 2017; Martin et al., 2017). Data protection is an element of cybersecurity and is the security assurances given regarding specific information contained within an IS. A business owner's application of data protection strategies means securing the most sensitive data in terms of the business missions.

The purpose of my literature review was to understand data protection. The literature included information on data protection in terms of regulation, threats, risks to sensitive data, how data is breached, the types of data lost, the processes to notify and recover data from a security breach, and the strategies used in data protection. My focus for the literature began with the conceptual perspective of ANT and the applications of its use within IS and IT research. My search efforts continued with an emphasis on current research associated with the elements of data protection. In the literature review, I provide a brief analysis of the importance of transitioning from an emphasis on protecting information systems containing data to protecting data, which was a foundational perspective of this study. The literature review also includes an analysis of alternative theories to ANT and rationale for not selecting them as frameworks for this study.

I collected literature that encompassed books, a proceeding, a working paper, multiple peer-reviewed journals, several dissertations, several executive orders, an enacted law, government websites, and selected government reports. I determined two overarching themes from my synthesis of the literature centered on prevention and

response associated with subthemes of regulatory, risks, breaches, loss, recovery, and the specific aspects of data protection. I obtained electronic information from databases residing within Walden University Library. I used Academic Search Complete, ACM Digital Library, Business Source Complete, EBSCOhost, ProQuest Central, SAGE Premier, SAGE Journals, Science Direct, and Taylor and Francis Online to comprise my scholarly review of the professional and academic literature on data protection.

The search criteria included the keywords *5G technology actant, actor, actor-network, actor-network theory, cloud-based computing, computer, computer security, cyber security, data, data breaches, data loss, data prevention, data protection, data response, data risk, data security, data theft, design, hackers, hacking, information, information loss, information security, Internet of things (IoT), regulations, security, sectoral law, unified law, United States, and qualitative*. The literature review contains a total of 120 references. Of these sources, 96% are peer-reviewed, and 88% (97) appear in published works from 2015 through 2019.

### **Actor-Network Theory (ANT)**

A conceptual framework in research is used to make sense of the findings. The ANT is a conceptual framework with previous research applications in sociological and technological environments. For example, ANT can be used in sociology by evaluating interactions occurring between events and the entities involved in the events (Elder-Vass, 2015), though this depends on the investigator's ability to explain events based on interactions occurring with or without the investigator's presence (Elder-Vass, 2015; Latour, 1996). Iyamu and Mgudlwa (2018) also demonstrated the use of ANT as a guide

for analyzing the interactions of people and objects with health care data. The application of the ANT is supported by the fact that a key characteristic of ANT application is symmetry, which refers to treating people and objects as the same and means that all actants and actors from an analytical stance become equals (Kurokawa, Schweber, & Hughes, 2017).

The ANT can also be applied to the IS field. Mähring, Holmström, Keil, and Montealegre (2004) used the escalation theory paired with ANT and discovered unique aspects of ANT for improving IS research. One, ANT is a framework focused on understanding the *how* and *why* actors and actants translations evolve. Two, ANT framework is a tool for researchers to understand ideas and assumptions about a phenomenon early in the process (Mähring et al., 2004). Silvis and Alexander (2014) advanced the application of ANT as an IS research methodology in sociotechnological research by using a graphical syntax tool to translate sociological and technological interactions. Additionally, Cavalheiro and Joia (2016) used the ANT concepts of problematization, interessement, enrollment, and mobilization as an analytical guide to provide awareness of gaps in hardware, software, and human skills that prevented a successful transformation to e-government technology. The ANT was an acceptable framework to explain the sociotechnological convergence of the network influences within data protection network assemblages.

Using the ANT in IS research has revealed benefits and limitations. One benefit of ANT is having a different conceptual framework for conceptualizing issues in IS research from more common approaches (i.e., systems theory). The ANT is distinct from

systems or systems thinking theory, which emphasizes the interactions of things with their smaller homogenous parts. In contrast, ANT is the focus on associations between assemblages (i.e., things) of a network (Elder-Vass, 2015; Jackson, 2015; Law, 2008). Assemblages are heterogeneous elements intertwined together without a static shape that influence interactions (Jackson, 2015). For example, the ANT introduces the concept of an actor network assemblage (Aradau & Blanke, 2015). This concept can be applied to data protection with the use of algorithms to address data-security assemblage based on knowledge of the systems and the people managing the systems (Aradau & Blanke, 2015).

Researchers have also expressed benefits from using ANT to introduce key concepts with translation of data protection assemblages (see Jackson, 2015; Kurokawa et al., 2017). The key elements of ANT (i.e., actants, actors, networks, translation, quasi-objects, problematization, interessement, enrollment, and mobilization) have simplified understanding of sociotechnological research findings (Jackson, 2015). The ANT has also simplified complexities between the sociotechnological aspects of science and technology (Iyamu & Mgudlwa, 2018), which supports its use as a framework extending to a sociotechnological study. The theory's concepts help researchers apply equally scientific claims to all components of the research to include human and nonhuman aspects involved in the phenomena (Kurokawa et al., 2017). In this study, I benefited from ANT as a framework for a vocabulary to capture network assemblages used in data protection. The use of the ANT framework in previous IS research furthered the

understanding of the sociotechnical and political processes involving data protection, business leaders, and information systems.

The ANT provides a simplified conceptualization of an investigation into technology and data as an actor. For example, Burga and Rezania (2017) related the factors of project governance, management stakeholders, and control and monitoring systems to data protection as actors and actants. Cavalheiro and Joia (2016) established a European patent office, Brazilian government, information systems, and patent data as actors and actants within an e-governance system. The study of patient experience data is another example of defining actors as bureaucratic documents, policies, and technologies (Desai et al., 2017). Based on this conceptualization, the ANT can be used for discovering connections between networks. For example, Iyamu and Mgudlwa (2018) demonstrated how the interactions move from individuals and objects to the agency of a network or groups of both. Further, the ANT provides vocabulary to interpret both phenomena (see Silvis & Alexander, 2014).

Another benefit is that ANT, as a social theory of technology, is a pathway for IT and IS researchers to understand a multitude of phenomena on how humans create or impact society through technology. For instance, Akhunzada et al. (2015) used the theory to address the complexity of humans influencing technology associated with data protection from the perspective of the threat. Jackson (2015) furthered this concept and reflected on the benefit of studying humans and non-humans equally from a combined social and technological approach. In IT research, many theorists do not address technical and social aspects of IT, instead research is conducted with a singular focus on social

aspects (Hanseth, Aanestad, & Berg, 2004). Baron and Gomez (2016) substantiated this view through a historical and conceptual development of ANT as a sociotechnological construct. ANT is an opportunity for a researcher to view the relationship between technology artifacts and the technological aspects (Hanseth et al., 2004). The ANT as a conceptual approach is a tool to understand societal and technological entanglements in sociotechnical networks and how these networks communicate on multiple sociotechnical networks (Baron & Gomez, 2016; Hanseth et al., 2004).

The ANT framework is beneficial, limitations exist within the application. One minor limitation of the ANT framework is the continued challenges against the use of it as a conceptual framework. For example, Elder-Vass (2015) argued the ANT framework when used conceptually contains gaps with the inclusion of people as part of the groups (i.e., assemblages). People are an important as a source of action for the actors and actants that comprise assemblages (Callon & Law, 1997). A researcher may evaluate people separately from information systems or vice versa, but the conclusions are meaningless for understanding sociotechnological networks if the people were not evaluated as part of the entire network (i.e., people and IS). Unless the interactions of people and information systems are investigated simultaneously within the heterogenous assemblage—relationships between different elements of a network (Vicsek, Király, & Kónya, 2016)—then the premise of the framework is uncorroborated (Jackson, 2015). In a heterogenous assemblage, the action of the relationship motivates elements of the network and causes an effect to the network (Sayes, 2014). This key premise is the

differentiator of the ANT framework when compared with systems or game theory, but it is also this principle that limits the use of ANT framework in IS/IT research.

The dual use of ANT as a conceptual framework and a methodology also poses a limitation. Silvis and Alexander (2014) combined their approach of ANT as a theory and a framework and influenced the interpretations from the research. But a potential limiting factor is an accurate translation of the roles of the actor-network established for the research (Cresswell, Worth, & Sheikh, 2010). For example, a researcher can use ANT to identify people and nonhuman systems interactions but not acknowledge the success or failure of the person's interaction with the object (Kurokawa et al., 2017).

Despite limitations of the theory, the ANT is a practical, conceptual framework for understanding complex data protection challenges. Hospitals, governments, and construction industries are examples of different industries faced with complex data protection challenges. For instance, Cresswell et al. (2010) evaluated health services, IT systems research with ANT, and determined that actors and actants within a network may influence other networks simultaneously based on the context. This demonstrates the concept of multiplicities. Researchers using ANT must understand the implications behind multiplicities and the existence of network layers (Cresswell et al., 2010). As multiplicities exist within layered networks, the defined roles and responsibilities of actors and actants are used by researchers to discern the context (Cresswell et al., 2010; Jackson, 2015; Silvis & Alexander, 2014). IT systems are an example of multiplicities with some users of the system functioning as administrators or architects of the system

infrastructure (Cresswell et al., 2010). Each role of a user created a multiplicity of the network altering the assemblage.

The ANT can be an alternative decision-making process that emphasizes the importance of certain actors who may be overlooked in traditional research frameworks (Desai et al., 2017). The ANT can be used as a conceptual approach to optimize examination of complex micro-level sociotechnical processes between actors and actants within an environment at a point in time (Kurokawa et al., 2017). Understanding the above points, ANT was an appropriate framework for realizing decision-making in developing data protection strategies.

### **Data Regulation**

The United States currently lacks a unified law for data protection. In the United States, individuals and entities apply a sectoral approach to data protection laws and regulations based on private sector trends regarding data protection (Diorio, 2015). The U.S. Code of Federal Regulations lists many acts designed to protect an individual's or entity's privacy associated with data but only when a specific action or precedence mitigates protection (Diorio, 2015; Office of the Law Revision Counsel, 2018a). The U.S. Constitution lacks a specific right to privacy, only provisioning terms that imply privacy rights are contained within the U.S. Constitution (Office of the Law Revision Counsel, 2018b). Other countries have a different approach to data protection laws such as unified data protection laws like the European Union GDPR (Diorio, 2015). The GDPR is a single unified law for EU citizens that applies to many online businesses around the world to consider *privacy by design*, entailing privacy rights designed within



information and communication technology from the initial concept of the information and communication technology system (Koops & Leenes, 2014). This lack of a foundational constitutional right to privacy correlates to a society that self-regulates their data protection. For business leaders, this necessitates developing data protection strategies not based on data protection law but an ad hoc basis against the threats to their data.

The deficiency of an overarching data protection law has led to multiple regulations addressing specific aspects of data protection. Like cybersecurity, many of the laws address enforcement actions, recovery notifications, or monetary penalties for the use of data in malicious practices (Schubert, Cedarbaum, & Schloss, 2015). For example, Senator Blumenthal introduced a new regulation into the Senate in 2017 detailing data breach accountability and enforcement for the protection of data (S. 1900, 2017). This proposed regulation is targeted at persons or businesses that handle or require, maintain, or use sensitive data (e.g., PII). These private and public entities must develop cybersecurity policies and procedures for the protection of the data in their possession (Data Breach Accountability and Enforcement Act, 2017).

In contrast, the Federal Information Security Modernization Act (2017) is a law that requires government agencies to have protections against cyberattacks. Other examples of ad hoc laws that emphasize oversight regarding sensitive data are the Federal Trade Commission Act (2017), the Health Insurance Portability and Accountability Act (2017), the United States Privacy Act (2017), and the Safe Harbor Act (2017). There is no one regulation specific to the act of protecting data from cyberattacks. The newly

introduced data breach accountability and enforcement bill, if passed, will signify a change of focus from more than cybersecurity to an emphasis on data security.

In the absence of a unified data protection law, business owners relying on ad hoc regulations refer to regulatory and nonregulatory agencies for data protection standards. In the absence of adequate data protection laws, agencies voluntarily seek out ways to improve data protection (Sarabdeen & Moonesar, 2018). This is emphasized by President Trump, who issued Executive Order No. 13800 directing all federal agencies to manage cybersecurity risks to their respective enterprise systems (Executive Order No. 13800, 2017). The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity publication is now the lead standard in data security following the issuance of the executive order (NIST, 2018). NIST personnel function as collaborators and facilitators to establish NIST standards, guidelines, education, and training (ITL Bulletin, 2012). To define data regarding BCI, businesses need an understanding of the data in association with the respective law or standard (Rumbold & Pierscionek, 2018). In essence, the lack of an overarching data protection regulation and implementation of ad hoc regulations necessitated businesses voluntary application of data security controls and protection strategies.

In a more recent move toward regulation as a requirement for data protection, as opposed to the voluntary application of data protection, the U.S. government is attempting to standardize the handling of unclassified information. President Obama signed Executive Order No. 13556, *Controlled Unclassified Information* (CUI), with the goal of providing federal agencies an initial legal framework to achieve standardization

of CUI (Executive Order No. 13556, 2010). To compliment this executive order, federal agency leaders worked with the executive agent of CUI, National Archives and Records Administration, and NIST to develop or use previously developed publications for distributing policy frameworks to assist nonfederal business leaders with the implementation of CUI requirements. The importance of these recent actions by the U.S. government is the acknowledgment that the nation's critical business data, which is the basis of U.S. competitive technological advantage, is threatened and requires a new mindset in the way data is handled and protected.

### **Data Threats**

Data threats and vulnerabilities are persistent and evolving. A security threat is a potential exploitation of data exposing vulnerabilities as weaknesses (Kaukola et al., 2017). Threats are sophisticated and customized to circumvent established security controls or protection methods (Baskerville et al., 2014). Data theft is a persistent threat to a company's personal information on their customers (Hinz et al., 2015). Hutchins et al. (2015) defined threat as an item that signifies potential impairment to another person, place, or thing. Kaukola et al. (2017) explained that business-critical information (i.e., proprietary, sensitive, or not) is subject to persistent and advanced persistent threats (APT; i.e., those threats to data on information systems over a longer period). National Cybersecurity Center of Excellence Information Technology Lab presenters posited the challenge for business leaders is balancing technology, growth, and innovation (Kauffman, Lesser, & Abe, 2015). The challenge is with maintaining an understanding of the changing threat landscape and protection strategies available for protecting data

(Kauffman, Lesser, & Abe, 2015). Hintze (2018) distinguished organizations as the controllers of data and third-party to the other firms functioning as the processors of the data. From these categorizations, understanding the threat is relegated to a firm's understanding of the complexities associated with the movement of data, data at rest, and the protection of data to meet compliance requirements (Calvard & Jeske, 2018; Hintze, 2018).

**The human threat.** Humans are one of the greatest threats to data. The human mindset contributes to how data security is regarded (Kaukola et al., 2017). Mindsets manifest as perceptions of risk or value regarding the data (Kaukola et al., 2017). The human mindset is a compounded threat to data when technology and security are required (Akhunzada et al., 2015). Connolly, Lang, Gathegi, and Tygar (2017) demonstrated how applications of technology and security techniques are a direct result of human behaviors regarding procedures. Connolly et al. indicated security procedure gaps related to human behavior might influence adherence to data security. Jenkins, Grimes, Proudfoot, and Lowry (2014) correlated this concept with the vulnerabilities of passwords and human behaviors towards security controls. Bonneau, Herley, Van Oorschot, and Stajano (2015) captured the weaknesses in passwords as a divergence between the theory of protections and the reality of practice. Compound these technology and security technique applications with data complexities, competing priorities, labor turnover, burnout, staffing, decision making, and a business leader's capability to manage data is a direct result of human error (Calvard & Jeske, 2018); indirectly this human error increases vulnerabilities and risks to data.

The human threat factor is important to understand from the perspective of intent. The human threat factor encompasses insiders and outsiders (Padayachee, 2016). Padayachee (2016) contended that opportunity is a dividing factor for outsider and insider threats. This division means outsiders need a vulnerability to threaten an information system (Padayachee, 2016). From the perspective of outsiders, these are the hackers responsible for cyberattacks (Bashir, Wee, Memon, & Guo, 2017). A hacker is an individual with malicious or non-malicious behavior profiles (Bashir et al., 2017). The hacker's intent is to gain technical or physical access to a digital environment using knowledge obtained by illegal methods to infiltrate or compromise security (Bashir et al., 2017). Examples of human mindsets grounded with ill intent are Man-at-the-end (MATE) and remote-MATE (RMATE; Akhunzada et al., 2015). A person's intent translates to different threats and risks for data security controls and protections (Bashir et al., 2017). The complimenting factor to a person's intent is a propensity to mindsets of efficacy, vertical individualism, and self-control (Bashir et al., 2017). These mindsets are an indication of a human's propensity towards hacking (Bashir et al., 2017). Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) posited a direct connection between non-compliant human behaviors with employee knowledge, attitude, and behavior when associated with an organization's security program. Connolly et al. (2017) indicated that employee intent is influenced by procedural security countermeasures and organizational culture. These values are causes for negative security behaviors within a task-oriented organizational culture (Connolly et al., 2017).

**Insider threat.** Directly connected with human behaviors and intent is the insider threat. The insider threat is a growing human-based vulnerability with data control (Tu, Spoa-Harty, & Xiao, 2015). The insider threat is an individual's use of their privileged access to an organization's data or the systems where the data resides, to knowingly or unwittingly, cause harm (Center for Development of Security Excellence, 2018; Padayachee, 2016). Defense Security Service specialists identify abnormal human behaviors as a cause for a potential insider threat (Center for Development of Security Excellence, 2018). Opportunities for insider threats arise from daily activities, valuable, visible, accessible, and transferable data assets, as well as technological innovations and changes (Padayachee, 2016). An insider vulnerability is the weakness created when an organization's capability to monitor the insider is lacking or non-existent (Tu et al., 2015). The existence of a potential insider threat means business professionals must understand the vulnerabilities to PII, BCI, or technologically valued data and mitigate those risks (Hubaux & Juels, 2016). J.-S. Wu et al. (2015) identified a link between corrupt human behaviors associated with data risk and loss referred to as data leakage. Business leaders understanding the human implications with data protection might make more informed decisions with data security.

**The data portability threat.** Business leaders are facing an evolving threat on a global scale known as data portability. Data portability is a new right established with the implementation of the GDPR (Mitchell, 2016). Data portability is the data subjects right to privacy, protection of personal data, and control over their data (Ursic, 2018). As mentioned earlier, the writers of the GDPR identified data controllers and data

processors, each having specific rights associated with data portability (Vanberg, 2018). Under the GDPR, a controller or processor may be an individual, a group, or an organization (Vanberg, 2018). The key point of the data portability right is that a data subject is authorized to direct a controller to transmit the data in question to another controller or processor (Engels, 2016).

The data portability right is a shift in how corporations approach securing data. Mitchell (2016) described the data portability right as a shift from corporations securing big data reservoirs to firms using a decentralized, distributed infrastructure approach in managing consumer data. Data security from the latter approach is now an issue for business leaders in determining how to improve data protection to minimize or avoid the risks and liabilities associated with possessing and transmitting a subject's data (Mitchell, 2016). Mitchell surmises the risk as a determination of retaining and maintaining personal data or creating portals of access to data. Engels (2016) and Mitchell captured the evolving threat as an impact to innovation and competitive advantage. Engels and Mitchell rationalized that a competitor indirectly gains access to another competitor's data under the GDPR data portability right.

**Future threats to data.** Future threats to business and personal data categories consist of cloud-based computing, the Internet of things (IoT), and 5G technology. These future threats require complex security solutions to implement improved data protection (Au, Liang, Liu, Lu, & Ning, 2018; Chaudhary, Kumar, & Zeadally, 2017; Choi, Yang, & Kwak, 2018; Fan, Ren, Wang, Li, & Yang, 2018; Jadhav et al., 2017; Suomalainen, Ahola, Majanen, Mämmelä, & Ruuska, 2018). Business professionals and individuals

must understand the security complexities required to implement evolving data protection schema.

**Cloud-based computing.** Cloud-based computing has created a target rich environment for hackers to obtain BCI and personal data. The centralized architecture of cloud-based computing, by which businesses and individuals store or access data, is a central issue for implementing a practical protection method (Yan, Li, & Kantola, 2015). Chaudhary et al. (2017) explained the bi-directional flow of information between geo-distributed systems presents another set of challenges for businesses. Au et al. (2018) focused on the problems with data protection in mobile cloud computing (i.e., the use of cloud-based computing from mobile devices) that included issues with authentication, encryption, and data integrity. Business leaders may realize cloud-based computing benefits from decreased storage costs and increased storage capabilities. However, the increased mobility coupled with the demand for access is creating complex issues for securing data.

**Internet of things.** IoT are individual devices with specific functions connected to the Internet with their own Internet protocol (IP) address through a distributed infrastructure (Chaudhary et al., 2017). Choi et al. (2018) identified gaps (i.e., lack of efficient security of user data) in the security by design associated with the implementation of IoT devices. The device makers overlooked the protection of data within the software platforms. This oversight has increased vulnerabilities and opportunity for hackers. Au et al. (2018) corroborated the weak security by design and the increased amount of IoT (e.g. 1.9 billion mobile devices by 2018) will compound the



challenge of data protection. As IoT increases virtualization and enables transfer of information between machines (e.g., machine to machine learning) the potential for malicious based threats to the data within the devices exponentially increased (Chaudhary et al., 2017; Choi et al., 2018; Jadhav et al., 2017). Chaudhary et al. (2017) explained that 50 billion IoT devices will exist and connect to the Internet by the year 2020. Choi et al. reported the increase of security vulnerabilities from six reports in 2014 to 362 incident reports in 2016 with most incidents associated with broadband devices. Popescul and Radu (2016) outlined the IoT vulnerabilities as insufficient password complexities, weak account enumeration, unencrypted network services, and user interface security concerns. Choi et al. outlined additional vulnerabilities associated with administrative processes, Internet, cloud, and device interfaces, mobile applications, coding issues, and device firmware and software updates combined with the lack of or weak update processes. Cloud-based computing and IoT are subordinate technologies within the world wide web that will advance as 5G technology develops.

**5G technology.** The fourth generation (4G) of wireless technology in 2018 is reliant mainly on operators, end users, and service providers monitoring information systems and mitigating threats through encryption technology (Fan et al., 2018; Suomalainen et al., 2018). Traditional cryptography for encryption is derived from the computational complexity associated with keys (Y. Wu et al., 2018). Smart devices with 5G technology are capable of computational capacities to overcome 4G encryption (Y. Wu et al., 2018). Fang, Qian, and Hu (2018) noted four crucial threats with 5G technology: (a) eavesdropping and traffic analysis, (b) jamming, (c) denial of service

(DoS) and distributed denial of service (DDOS), and (d) man-in-the-middle (MITM) attacks.

***Data protection strategies in the future threat environment.*** As the world moves from 4G to 5G, data protection is a present-day and future problem for business leaders. Chaudhary et al. (2017) proposed integrating software-defined networking (SDN), network service chaining (NSC), and mobile edge computing (MEC) to create a secure infrastructure for data exchange with evolving technologies like cloud-based computing. Y. Wu et al. (2018) worked with physical layer security to improve data protection in cloud-based and IoT computing. Au et al. (2018) argued data protections in cloud-computing, specifically mobile devices uploading to the cloud, require a focus on user-centric behaviors in the areas of identity authentication, data encryption, and data integrity check. Au et al. recommended these types of data protection strategies based on biometric-based authentication, symmetric and asymmetric encryption (i.e., advanced encryption standard [AES] or public key encryption [PKE]), and the use of audio, video, and bio-based data integrity checks. Yan et al. (2015) discussed symmetric and asymmetric encryption as beneficial to data protection in cloud-computing. However, it is recommended to use proxy encryption through reputation centers as an alternative method in data protection for cloud-computing (Yan et al., 2015). Reputation centers are a method based on a cloud-computing service center reputation and that of the data requestor. Business leaders need to understand their data to determine the best strategy to prepare for the future threat environment.

Ultimately, business leaders must understand threats to their data to determine vulnerabilities associated with the data to administer an acceptable risk tolerance approach. Threats are sophisticated and customized to circumvent the established threat control processes (Baskerville et al., 2014). Unmitigated threats lead to increased risks affecting a company's costs, reputation, performance, and competitive advantage (NIST, 2018). The problem with understanding threats is people, processes, and technology comprise the threats. The complement of this problem is the security protocols executed as countermeasures to the threats are executed by people, or through procedural modifications, or with technological innovations, changes, and efficiencies. Business leaders require continued focus on identifying threats to their data to ensure an appropriate risk tolerance approach.

### **Data Risk**

Different threats translate into different vulnerabilities that impact the types of risks to a firm's data. Hutchins et al. (2015) defined risk as an undesirable outcome of an event. Aven (2016) explained risks as an uncertain event linked to the probability of loss or damage to a business asset. Some ME rely on the experience of their leaders and staff to predict risks (Naude & Chiweshe, 2017). Naude and Chiweshe (2017) posited a risk management framework tool for ME businesses to manage risk identification, assessment, mitigation, and monitoring. Lavastre, Gunasekaran, and Spalanzani (2012) and Blome, Schoenherr, and Eckstein (2014) identified operational risks affecting ME as weak alignment to business strategies, adherence to imposed regulatory requirements, dynamic consumer preferences, low or missing employee skill sets, unreliable or lack of

vetting vendors and suppliers, economic impacts, technological, social aspects, weak infrastructure of IS/IT equipment, and natural disasters. Yahoo organizational leaders and stakeholders compounded their pre-existing risks with a failure to make cybersecurity a strategic priority (Whitler & Farris, 2017). Yahoo leader's failures in strategic thinking exposed 1 billion user accounts and their respective data resulting in a stock market loss of 1.5 billion U.S. dollars. Businesses need standardized risk practices to decrease organizational risk and maximize cost savings (Hutchins et al., 2015). Many IS/IT professionals recognize risk as a function of threats and vulnerabilities.

### **Data Breaches**

James B. Comey, Director, Federal Bureau of Investigations, emphasized the fact that dealing with a data breach means understanding the impact specifically on the data (FBI, 2017). A data breach is a type of security incident that involves the unauthorized exfiltration of a firm's data by an attacker (Whitler & Farris, 2017). Kongnso (2015) analyzed the impacts of data breaches as financial, performance, and competitive advantage. Naude and Chiweshe (2017) contended that data breaches are responsible for greater operational risks with an ME that negatively affect production, expenses, and returns on revenues. The next step for businesses is evaluating how and why a cyberattack on the data occurs.

Business leaders might not understand the connections between data breaches and security controls or protections without evaluating how and why a cyberattack occurs. In a series of published academic research articles from 2014 through 2017, researcher findings noted business leaders that incorporated newer technology (i.e., social media and

cloud computing) with existing technological and security platforms experienced an increase in data breaches due to a lack of updated security measures to support the newer technology (Angst, Block, D'Arcy, & Kelley, 2017; Ashenmacher, 2016; Hemphill & Longstreet, 2016; Holt, Smirnova, & Chua, 2016; Layton & Watters, 2014). Layton and Watters (2014) noted businesses incorporating new technologies overlooked or minimized the laborious need for updated security controls to compliment the newer technology. The Target store data breach is an example of how the overlooked security controls resulted in negative impacts for data protection affecting over 70 million consumers and 40 million credit and debit card records (Foresman, 2015; Plachkinova & Maurer, 2018). Gwebu, Wang, and Wang (2018) used cognitive dissonance theory to understand how a firm's knowledge levels of available tools for preventing data breaches and safeguarding data impacted the firm's reputation and financial stability. When a firm's IT professionals employed response strategies, Gwebu et al. found these strategies provided increased data protection minimizing data breaches and financial impacts.

Business leaders' misunderstanding of the threat to their data might result in harm to the organization and the stakeholders. Ashenmacher (2016) examined the potential harm caused to consumers when entities incur data breaches and are unable to protect the PII. Holt et al. (2016) researched the cost earned on the stolen data (i.e., PII) by cybercriminals and the profit on the black market (i.e., open markets online). Like Ashenmacher and Holt et al., Hemphill and Longstreet (2016) and Angst et al. (2017) examined the security practices and theory established to prevent the susceptibility of data breaches over a specific period. Both Hemphill and Longstreet and Angst et al.

hypothesized specific characteristics of an organization's security standards minimized the potential occurrence of a data breach. Connolly et al. (2017) provided the example of how flat organizational structures, solidarity, and people-oriented cultures enabled information security standards and practices. A lack of security controls and protections are shown to increase the potential for data breaches.

Layton and Watters (2014), Hemphill and Longstreet (2016), Holt et al. (2016), and Ashenmacher (2016) research various aspects of data breaches. Layton and Watters evaluated and defined future data breaches and the impact to cost. Hemphill and Longstreet concentrated on the theory and practices established by the Payment Card Industry Security Standards Council (Council) that fights against cybercrime globally. Holt et al. reviewed the variety of profits made on the black markets through buyers. Ashenmacher researched statistics of stolen PII associated with data breaches. Angst et al. (2017) characterized the adaptiveness with the effectiveness of IT security investments in preventing a data breach. The trend with data breaches is businesses evaluated the cost regarding the least expensive route; protect against the data breach or spend in recovery costs.

The findings of the above researchers noted key themes. Angst et al. (2017) discussed how business leaders that symbolically adopted IT security, regardless of IT security investments made, faced greater chances of a data breach versus those business leaders with the rigorous adoption of IT security (i.e., substantive adopters). Hemphill and Longstreet (2016) recommended the Council improve the security standards and cyber liability insurance coverage as technologies advanced to ensure the protection of

consumers PII during data breaches. Similarly, Ashenmacher (2016) found the Federal Trade Commissions' (FTC) lack of enforcement contributed to data breaches and consumers with stolen PII. Ashenmacher noted with the FTC failing to enforce data security and ensuring the protection of consumer dignity; data breaches continued to result in hackers obtaining proprietary and consumer personal data. Holt et al. (2016) revealed that revenues earned from the stolen transactions were minuscule compared to stealing, selling, and using a consumer's identity. Layton and Watters (2014) discovered that data loss suffered from a data breach had a significant impact on a business' tangible costs. The firm leaders still operated successfully because the breach became a business write-off (Layton & Watters, 2014). The tradeoff for the business owner is to pay the loss sacrificing the lost data (i.e., PII or BCI) or protect against the potential of a data breach and reduce data loss.

### **Data Loss Prevention**

Businesses experienced data loss from internal and external threats to data. DLP personnel must address insiders and outsiders attacking their data to mitigate data loss. Arbel (2015) defined DLP as the detection of data in transit through system processes to prevent data loss. People prevent loss of data through the development and analysis of infrastructures regarding cyber threats and risks (Miron & Muita, 2014). Miron and Muita (2014) discussed the nature of DLP involving standards and controls to prevent future cyberattacks. Vitel and Bliddal (2015) used France's cyber defense to demonstrate the use of standards and controls in DLP. French cybersecurity professionals realized preventing data loss involved understanding the attacks through counter-attack

disciplines via online environments, cyber security levels, and increased knowledge of cyber-crimes. Plachkinova and Maurer (2018) used the Target data breach as a teaching case study to demonstrate how data prevention and response strategies improved customer loyalty, cybersecurity, chip readers. Plachkinova and Maurer demonstrated that the right leadership provided improvements and guidance for businesses practicing DLP. Arlitsch and Edelman (2014) expanded the idea of understanding cyber-crimes to the techniques used by the cyber attacker. Arlitsch and Edelman suggested simple best practices like (a) proper device management, (b) data stewardship, (c) password use and protection, (d) password vault software, and (e) personal monitoring of credit cards to prevent future cyberattacks.

DLP is a process of awareness in the physical protection of data, prevention of data loss, and response to data loss. The methods of DLP included data categorization, user profiling, and tracking and restricting data access (Arbel, 2015). In the case of the latter, IS/IT professionals rely on intrusion detection systems (IDS) to detect cyberattacks (Ben-Asher & Gonzalez, 2015). IDS is a system of generated warnings to enable network administrators the ability to thwart an attacker's control of the corporate network and prevent data loss (Ben-Asher & Gonzalez, 2015). When businesses failed to implement adequate DLP measures a data recovery plan became necessary.

### **Data Security Breach Notification and Recovery**

Data security breach notification was an expensive solution to DLP. The cost burden for data recovery is notification centric (Agelidis, 2016). Business leaders followed security breach notification laws that outlined the requirements for businesses to



make formal notifications to victims of data breaches (Agelidis, 2016). Approximately 47 states adopted security breach notification laws and experienced a decrease in the number of data breaches with a cost savings of 93 million dollars (Sullivan & Maniff, 2016). Sullivan and Maniff (2016) argued the concept behind the security breach notification laws is one of a legal duty for an organization to protect a consumer's data. After the Target data breach, Target representatives sent notifications to victims and offered 1 year free of credit monitoring services (Plachkinova & Maurer, 2018). The government representatives from the Office of Personnel Management (OPM) offered the 21.5 million victims of their data breach a similar option for 3 years of monitoring services at the cost of 133 million dollars (Gootman, 2016).

The OPM data breach indirectly impacted the entities outside of the victims and organizations related to the data breach (Hemphill & Longstreet, 2016). Target's data breach is another example of costs from data breaches impacting an organization indirectly. Target's supporting financial institutions lost 200 million dollars as opposed to Target's loss of 148 million dollars that was offset by the 38-million-dollar insurance payout the company received following the data breach (Hemphill & Longstreet, 2016). Whitley and Farris (2017) expounded on the hidden costs associated with image, branding, and reputation noting the negative effects from slow responses (e.g., Sullivan and Maniff [2016] noted an average of 117 days between breach and notification), deniability (e.g., Yahoo's failure to acknowledge the breach), lawsuits, and investigations. Businesses need to evaluate the repercussions of preceding DLP for

recovery actions as these direct costs, indirect costs, and hidden costs negatively affect financial solvency.

Data recovery is the second aspect of a business's response to a data breach. Businesses' ability to respond to data breaches is a key focus for many federal institutions (Pipelines, 2016). The Department of Transportation (DOT) is incorporating planning response as a strategy for their agency with protecting U.S. pipelines from cyberattacks (Pipelines, 2016). Organizations' computer response teams must establish data integrity as part of the recovery process (Agelidis, 2016). Plachkinova and Maurer (2018) explained how investigating a data breach is an important facet of recovery. Plachkinova and Maurer further explained how the purpose of the investigation is to identify weaknesses and improve those vulnerabilities. Gootman (2016) identified OPM efforts at data recovery involving a *Cybersecurity Action Report* with the assistance of external stakeholders to identify 15 strategies to improve data security. Businesses need to evaluate the cost-benefits of investing in security to prevent data breaches or the cost-impacts of investing in notification and recovery to respond to data breaches.

### **Data Protection**

Data protection involves a business leader determining the importance of BCI (i.e., a firm's most important data) or PII. Kaukola et al. (2017) defined BCI as the organizational data considered proprietary or sensitive and an asset to the firm that requires increased protection. Rumbold and Pierscionek (2018) posited a problem for businesses with data protection is the ability to distinguish between what are data and what is information. Rumbold and Pierscionek distinguished the relationship between

data and information as the context. An illustration of this problem may be demonstrated by the case of a scientist who analyzes raw data to form information for a purpose used in decision-making, innovation, and conclusions (Rumbold & Pierscionek, 2018). Data give value to information and to protect data business leaders must understand that informational value relative to their specific firm or organization.

Data protections evaluated regarding technical and organizational measures are commensurate to the risk (Hintze, 2018). Businesses need to assess the data as a function of threats and vulnerabilities through the confidentiality, integrity, and availability (CIA) principle to understand risk. CIA is a means to categorize consequences associated with the loss, compromise, or suspected compromise of data (Hutchins et al., 2015). Businesses determine the risk tolerance by evaluating the cost of data loss, compromise, or suspected compromise (NIST, 2018). Anugerah and Indriani (2018) recommended the development of data protection strategies based on the analysis of threats and risks regarding identification, detection, response, and recovery of the data.

A variety of major themes existed for data protection in academic research during the years 2016 through 2018; some researchers focused on individual data privacy protections relative to technological, methodological, and managerial aspects of data (Hardy, Hughes, Hulen, & Schwartz, 2016; Hubaux & Juels, 2016; Jackson, 2018; Kuang et al., 2018; O'Connor et al., 2017; Schneider, Jagpal, Gupta, Li, & Yu, 2017). Arguments and considerations associated with the release of the GDPR and the impacts to individual privacy are another area of focus in academia (Ceross, 2018; Kennedy & Millard, 2016), big data protection issues related to large-scale data analytics about

individuals and privacy when sharing the data (Altman, Wood, O'Brien, & Gasser, 2018; Iyamu & Mgudlwa, 2018), and the various data protection schema stemming from technological harms (Arlitsch & Edelman, 2014; Bonneau et al., 2015; Gellert, 2015; Ghafoor, Sher, Imran, & Derhab, 2015; Hubaux & Juels, 2016; Jenkins et al., 2014; Miron & Muita, 2014; Olaniyi, Folorunso, Aliyu, & Olugbenga, 2016; Parsons et al., 2014; Tanev, Tzolov, & Apiafi, 2015; Tu et al., 2015; Wang et al., 2017; Zuva, Esan, & Ngwira, 2014). These major themes are focused on the distinctiveness of data as a standalone element of IS and IT exposed to unique threats. Data, as an element, require tailored and specific protection against these unique threats with more rigorous controls than traditional cybersecurity protections.

Some researchers presented data protection schema focused on different aspects of data but not the protection of data itself as a foundational element of information. Genkin, Pachmanov, Pipman, Shamir, and Tromer (2016) discussed cryptographic software development grounded in theory to protect information systems against evaluating cryptography on specific BCI. Arlitsch and Edelman (2014) expanded the understanding of hacker techniques focused on data as an element of information. Arlitsch and Edelman (2014) indicated hacker techniques are an area of protection that must be considered for data at rest (i.e., stored data). Jenkins et al. (2014) identified keystrokes used in the development of passwords. Again, this is an area of protecting data at rest. Wang et al. (2017) evaluated data transmission and access protection processes. This research is primarily the understanding of data protection while data is in transit. Tu et al. (2015) conducted analyses of data protection within a medical enterprise but

narrowly focused on internal access data control mechanisms associated with insider threat. Zuva et al. (2014) tested facial and fingerprint technology to evaluate the accuracy of user identification. This narrow focus on user identification accuracy improved aspects of data protection for confidentiality and integrity. While the scholarly research on data protection was present, there was a limited amount of academic research specifically analyzing and understanding data protection strategies for data as the foundational element of information. More specifically for businesses, there are gaps in the research on data protection correlated to the protection strategies for BCI or PII.

Some researchers understood the necessities of evaluating data protection as a holistic concept for protecting against potential harms to data. Gellert (2015) defined harms to data in the age of advanced computer-based technologies in terms of the increased data amounts, greater access to the data, and data as a technological means to manage society. These harms are noted as responsible for the additional problems: (a) a lack of trust at the individual level (i.e., due to the inaccuracy of data whether intentional or non-intentional), (b) the burden of proof for the accuracy in the data becomes an individual's responsibility, and (c) the potential for loss of control when data is accessed with or without intent is a concern for the data owner. Last, data becomes information within a digital system used to structure society through regulation and policy processes (Gellert, 2015). Hung (2017) applied the ANT to the understanding of protecting data as the whole network assemblages of humans and technologies, the translation of assemblages' interactions, and the multiplicity of other actor-network assemblages influencing the network outcomes. Using a gaming software environment, Hung

demonstrated the *how* and *why* of player strategy selection in protection schema to counter constraints, challenges, and opportunities to the sociotechnological environments of the game assemblage. Fielder, Panaousis, Malacaria, Hankin, and Smeraldi (2016) pursued a similar viewpoint with decision-making models in understanding vulnerabilities and risks to data to mitigate the costs of data loss. Cresswell et al. (2010) illustrated the importance of data as a record influencing the relationships between humans and non-humans with the ANT as a framework. Cresswell et al. demonstrated the value of the ANT in the context of micro aspects of an environment to translate or infer an understanding of macro complex social processes. The importance of the research denoted above is the evolution from protecting information systems to the foundational level of protecting data.

### **Alternative Theories**

I researched several alternative theories (i.e., moving target defenses, systems theory, and systems thinking theory). Zhuang, Bardas, DeLoach, and Ou (2015) developed a theory of cyberattacks relating to moving target defenses. Zhuang et al. postulated moving target defenses theory as a game changer for cyber security by establishing a framework for continually changing defenses versus using static defenses. The theorists of moving target defenses theory acknowledged the ongoing need for further support of the newer theory (Zhuang et al., 2015). Due to the novelty of moving target defenses theory, I pursued a more established conceptual framework within ANT.

Salim (2014) presented a working paper that discussed cyber safety using systems and systems thinking theory. Salim argued cyberattacks continued due to the belief by

business owners that jurisdictions exist in the cyber world. Attackers operate without geographical boundaries with the support of an underground economy. Salim theorized cybersecurity as imperceptible through physical means alone recommending IT leaders require a holistic approach. IT leaders embracing a holistic approach for countering attacks required technical and nontechnical protection methods (Salim, 2014). A comprehensive examination of technical (i.e., data protection methods) and nontechnical (i.e., people) interactions offered a complicated but feasible approach. ANT provided a simple framework to understand all variables in the problem as actors and actants regardless of whether the actor or actant is human or non-human.

Similar to Salim (2014), dissertations on cybersecurity published between the years of 2015 through 2017 used general systems theory focused on the protection of information and the systems housing the data (Cook, 2017; Kongnso, 2015; Saber, 2016). Cook (2017) framed the investigation into effective strategies small to medium-sized (SMEs) businesses used to protect themselves from cyberattacks by using the general systems theory (GST). Von Bertalanffy (1968) envisioned systems theory as a means for characterizing the interrelationships between modules of systems versus the individual modules. Systems theory is expanded by Kuhn (1970) to capture the procedural aspects of systematically increasing knowledge through scientific discovery. Cook's premise is that people facilitate cybersecurity through strategies, procedures, risk assessments, and efficient network protocols (i.e., a systematically secure operation). Kongnso (2015) evaluated cybersecurity best practices for minimizing data breaches using general systems theory. Saber (2016) investigated the cybersecurity strategies associated with

protecting information systems from data breaches within the framework of general systems theory as well. Saber provided an additional framework for the qualitative exploratory case study to explore cybercrime activities using Cohen and Felson's (1979) routine activity theory.

Sayin (2016) presented the requirements for converting systems theory to a social context. A critical component of the conversion rests with identifying the human errors within the social system (Sayin, 2016). For a successful conversion, a decrease in human error must occur for the system to remain viable (Sayin, 2016). The concern with the selection of a systems theory framework is the division created by identifying all the elements as unique entities (Sayin, 2016). General systems theory and routine activities theory share a similar characteristic in that each evaluates cybersecurity through a human lens. This characteristic is also a gap. The gap in the research with understanding the dynamics between human and non-human interactions as a sociotechnological assemblage (Jackson, 2015). ANT is a framework offering an analytical approach beyond the human-centered view (Jackson, 2015). The application of the ANT framework decreases a gap in information systems based research.

### **Transition**

In Section 1, I provided the objectives of my study. The objectives included the identification of the problem, purpose, and nature of the study. I detailed the potential outcomes and benefits of this study with the business impact and significance of this study. Section 1 concluded with a professional and academic literature review.



Section 2 contains a restatement of the study purpose with comprehensive details of the project. These details include the role of the researcher, the participants, research methodology, and design of the study in greater detail. I also discuss the population and sampling criteria, data collection instrument, techniques, organization, and analysis methodologies. Section 2 concludes with reliability and validity criteria as well as a transition from Section 2 to Section 3. Section 3 will encompass an analysis of the findings from the research conducted in this study. Topics in Section 3 will evaluate the applications to professional practice and implications for social change.

## Section 2: The Project

My review of literature in Section 1 provided a synthesis of ANT, the elements of data protection, the supporting themes on protecting data as the critical component of information, and contrasting theories used in previous IS/IT research. The literature also indicated a gap in research regarding data protection strategies as a foundational element of BCI. As virtualization grows from 1.9 billion mobile devices in 2018 to 50 billion devices by 2020, the dependence on wireless technology drives an increased threat environment within these complex networks (Au et al., 2018; Chaudhary et al., 2017; Y. Wu et al., 2018). My objective with this study was to explore the effective data protection strategies ME business leaders use to improve data protection to reduce data loss from cyberattacks.

Section 2 is a presentation of the research method, design, the role I played as the researcher, the selection requirements for the participants, and the characteristics of the population and sample for the conducted study. I also provide a discussion of the ethical requirements regarding this research and details surrounding the data collection. The data collection details include the instruments, techniques, organization techniques, analysis, reliability, and validity to support the selected method and design of this study.

### **Purpose Statement**

The purpose of this qualitative, single case study was to explore the strategies that ME business leaders use to improve data protection to reduce data loss from cyberattacks. The targeted population for this study included three ME business leaders from a global worldwide services company in Brevard County, Florida. These ME business leaders

implemented strategies that improved data protection and reduced data loss from cyberattacks. Business leaders' acceptance of the study's findings might spread the use of effective strategies for reducing data losses and recovery costs. ME owners reducing data loss from cyberattacks can contribute to positive social change by altering attitudes toward data protection, reducing costs associated with protection against Internet crimes, and enhancing an individual's capabilities in the protection of sensitive, proprietary, and PII.

### **Role of the Researcher**

Defining and describing the role of the researcher in the data collection process is important in research (Heeney, 2017). As the primary data collection instrument, I interpreted the interactions of the actors and actants in this case study. The role of the researcher is not to solve problems associated with the interactions occurring in the study (Heeney, 2017). In qualitative studies, the researcher's role also includes eliciting meaning from within a bounded framework (Sarma, 2015). For researchers applying an ANT approach, the focus of the research is important to define within the context of the study to minimize the multiplicities; for example, researchers may investigate the wrong phenomena by following an associated actor-network (i.e., a multiplicity) versus the primary actor-network (Cresswell et al., 2010). Researchers must define their role with an accounting of themselves in the network of study, which may be as an actor or actant (Cresswell et al., 2010; Heeney, 2017; Silvis & Alexander, 2014). I assumed the role of primary data collection instrument and established this context for the ANT framework and boundaries within this study and my delimitations.

I balanced my role as a researcher with the relationships involved in participant-based research. For instance, researchers as interviewers require rapport to encourage exploration with interviewees (Newton, 2017). My experience with data protection includes over 20 years of information security with 10 years managing and securing data with the Department of Defense. This experience includes investigating, interviewing, and coordinating personnel to determine the impact on contractor and Department of Defense IS from data breaches, misuse of digital data, and instances of the loss of physical and digital data. From 2008 to 2010, I spent 2 years working with the Department of the Army investigating data spills for IS maintaining national security information. As the researcher and interviewer, my knowledge of data protection enabled proper reporting and definition of the activities within the ANT framework. A researcher conducting research under the ANT framework must ensure several aspects of the ANT framework are applied to a study: (a) the definition of the nature of the problem (i.e., problematisation), (b) the roles of the actors and actants (i.e., interressement), (c) the strategies for interrelations between the actors, actants, and roles (i.e., enrollment), and (d) the methods of input to ensure the participants providing input about the activities are well-informed (i.e., mobilisation; Jackson, 2015). I possessed the appropriate knowledge and skills to execute the requirements of the researcher role within the ANT framework for the executed this study.

Another part of my role pertaining to this research is one of ethics and specific protections afforded to human participants. It is important to identify ethical issues in empirical research, and the researcher has a role to capture activities without judgment

while protecting the participants (Heeney, 2017). I reviewed *The Belmont Report* regarding the principles of ethics and the protection guidelines for human subjects in research (Office of Human Research Protections, 2016). Ethical standards are the foundation for research processes and treating participants with respect through the research upholds ethics within the study (Ngulube, 2015). The ethical guidelines are established to ensure fair practices in research, equitable distribution of benefits and burdens, and for the safety and wellbeing of participants (Brody, Migueles, & Wendler, 2015). I accomplished the National Institutes of Health Office of Extramural Research certification. I understood that maintaining high-quality research included an ethical approach that protected human participants.

I mitigated bias and avoided viewing data through my personal lens or perspective. It is important to make sense of the participants' experiences filtered through the researcher's view but not altered by the researcher (Yazan, 2015). There are three aspects of bias with a researcher's interpretations and objectivity that must be mitigated (Neusar, 2014). First, a researcher mitigates bias by recognizing their individual values and ideologies and segregating those views from the views of the interviewee (Neusar, 2014). Second, a researcher mitigates bias through factual writing and avoidance of persuasiveness within the writing (Neusar, 2014). Third, in a case study that involves less than a few companies, variability of the sample is incorporated through understanding generalizations of the sample (Neusar, 2014). The mitigation of bias was supported through research protocols.

I also used interview and journaling protocols to mitigate bias and aid validity and reliability. The interview protocol was a guide for obtaining relevant information within a scripted process and with assuring participant confidentiality obtained through informed consent (Dikko, 2016). It is also important to ask questions relevant to the research topic (Ngulube, 2015). The elimination of leading questions during the data collection process minimized the potential for bias and increased the validity of the research (Onwuegbuzie & Hwang, 2014). An interview protocol with semistructured interview questions was an optimal means of gaining rich data (Dikko, 2016). A researcher may interpret or construct a framework of the phenomena from the data collected to explore an understanding of the research problem (Ngulube, 2015). A researcher's memories from interviews can create bias, but this can be mitigated through journaling, writing down expectations, events, and ideas (Neusar, 2014). The use of interview and journaling protocols was a suitable strategy for mitigating bias and enhancing validity and reliability in my study.

### **Participants**

I selected participants with an established set of criteria to support the investigation of a deeper understanding of data protection strategies used in reducing data loss from cyberattacks. It is important to have involved or informed participants contributing to the phenomena being studied (Johnson et al., 2017). Purposeful sampling is used to select individuals who possess the knowledge, experience, and ability to communicate on the phenomenon of interest (Boddy, 2016). It is also important that study participants can support the purpose of the study and elucidating answers to the

research question (Bengtsson, 2016; Dasgupta, 2015). The phenomenon of interest in this study was data protection strategies that reduce data loss. The research question for this study was “What strategies do ME business leaders use to improve data protection to reduce data loss resulting from cyberattacks?” A purposeful sample of ME business leaders with specific knowledge of data protection strategies that reduce data loss from cyberattacks was used for this study.

The characteristics of the ME were an important component in determining the participants. The ME was considered the unit of analysis and by understanding the ME the selection of participants can be determined for the study (Dasgupta, 2015). As this was a qualitative single case study design, the unit of analysis was one ME operating worldwide. I selected participants based on the depth of rich information rather than focusing on the number of participants (see Onwuegbuzie & Byers, 2014). A small number of participants associated with a location or organization in qualitative research does not negate the rigor of qualitative research (Sarma, 2015). I ensured that the selected participants were from within the selected ME. The ME business leaders possessed a baccalaureate or higher education in business or information management or were able to substitute the educational requirement with a minimum of 3 years working in an IT/IS related discipline for a department of defense contractor and 1 year or greater working specifically with protecting data for a cleared defense contractor.

I maintained professional associations with many defense industry businesses in Brevard County, Florida that required data protection as part of contractual agreements with the U.S. government. I gained access to potential participants within the ME using

my professional associations and personally visited ME businesses that met the unit of analysis characteristics. The participants were a small group of employees of the ME who were business leaders (i.e., a vice president, department manager, or team lead) and IT or IS professionals (i.e., members of the IT department or within the chain of decision makers for IT and IS). Homogenous selection is important in purposeful sampling to support the objective and strategy of the study (Palinkas et al., 2015). The objective of this study was to explore the strategies ME business leaders use to improve data protection to reduce data loss from cyberattacks. The sample size was determined by selecting participants possessing knowledge or experience of data protection strategies with evidence of a reduction of data loss from cyberattacks.

An approach to gaining trust and establishing rapport in qualitative research is communicating self-disclosure and confidentiality with potential participants. Researchers establishing trust and rapport tend to lessen issues arising from interviewing (McDermid, Peters, Jackson, & Daly, 2014). As mentioned, I maintained professional associations with many defense industry businesses in Brevard County, Florida. Potential participants may have known me through these professional associations. This preexisting relationship strengthened the trust and rapport already present.

I provided with my initial visits an informed consent, interview and journaling protocol, and developed initial interactions with the potential case study participants. This immediate approach in sharing the informed consent, interview, and journaling protocol was important for two reasons. One, it acknowledged to potential participants my understanding of a potential impact on them as a by-product of their possible



participation. Two, sharing these documents with potential participants clarified their rights to information and privacy associated with the study. It is important for participants to understand the insights they can provide and how they can contribute to the research (Lie & Witteveen, 2017). Providing documentation to potential participants regarding the aspects of no risk of harm also communicates respect to their values (Lie & Witteveen, 2017). I used face-to-face contact with the potential participants to exchange my e-mail and phone information, explain how I planned to execute participant informed consent form prior to the semistructured interviews, and to share the interview and journaling protocols.

## **Research Method and Design**

### **Research Method**

A qualitative method was used for this study. Researchers apply a qualitative approach in environments when inductive reasoning requires understanding the data associated with a newly developing phenomena (Graneheim, Lindgren, & Lundman, 2017; Yin, 2014). Further, the use of a qualitative method increases analytical flexibility in a social and bounded framework of the study (Yin, 2014). I used the qualitative method with multiple sources of data collection within set criteria to contribute to the truthfulness of the study (Sarma, 2015). Data patterns are the basis of the theoretical understanding of the problem being researched (Graneheim et al., 2017). I also chose the qualitative method because researchers choose methodology based on their study objectives, research questions, data collection, and time frames (Cook, 2017). A review of the literature indicated a lack of formal research into the successful applications of data

protection strategies in reducing data loss. Qualitative evaluation of the problem of data loss impacting businesses remains a developing issue for many business leaders and researchers, especially understanding how the human, procedural, and technological facets interact to assist business leaders with implementation of data protection strategies (Crowley & Johnstone, 2016; Dang-Pham, Pittayachawan, & Bruno, 2016; Hooper & McKissack, 2016; Parent & Cusack, 2016).

There are several reasons why researchers use qualitative inquiry for understanding phenomena. First, researchers use qualitative inquiry to interpret meaning with a problem to establish a theoretical foundation (Basias & Pollalis, 2018; Cibangu, 2013; Yin, 2014). Second, researchers rely on a qualitative approach to establish the specific knowledge context for transferability to a larger population (Cibangu, 2013). Third, researchers generalize meaning from subjective opinions, attitudes, beliefs, or experiences of a problem in a real-world context (Cibangu, 2013; Orlu, 2016; Percy, Kostere, & Kostere, 2015; Yin, 2014). With the lack of research specific to data as a foundational element of information requiring unique protections, a qualitative research approach provided a foundation for investigating data protection strategies.

A qualitative method supported my study purpose in exploring business leaders' choice of data protection strategies to reduce data loss succeeding a cyberattack, and it is a method that has been supported in previous research. For example, Orlu (2016) used a qualitative approach for exploration of student behaviors to explain the organized aspects applied with seeking information. Nassaji (2015) also demonstrated the descriptive characteristics of qualitative inquiry to find meaning in the natural context of language

learning without manipulation of variables present in the environment (i.e., language learning in a real-world setting). Further, Salviulo and Scanniello (2014) qualitatively observed software developers to gain knowledge of source code comprehension and maintenance. Finally, Yazan (2015) presented the work of three qualitative methodologists who shared a common conclusion regarding qualitative research method selection.

Researchers use quantitative and mixed-methods research for different purposes when investigating phenomena. Quantitative research comprises a statistical and testing approach to researching a problem for the formulation of a hypothesis (Hossain & Dwivedi, 2014). For example, Levi and Williams (2013) developed a hypothesis using multi-agency cooperation data and then quantified factors of cooperation frequency associated with cybercrime perceptions to test the hypothesis. Dadelo, Turskis, Zavadskas, and Dadeliene (2014) also used a quantitative approach involving statistical analysis of qualitative data. Evaluation in quantitative studies occurred through statistical manipulation of data (Dadelo et al., 2014; Hossain & Dwivedi, 2014; Levi & Williams, 2013). Another differentiator between a quantitative and qualitative approach is theory testing (i.e., quantitative) versus theory building (i.e., qualitative; Dasgupta, 2015). A quantitative method would have been appropriate for use if the phenomenon (e.g., data protection strategies in reducing data loss) entailed manipulation of the variables to support a model or hypothesis. I did not quantify the phenomenon of data protection strategies in this study, so I chose a qualitative method.

Researchers achieve balance with a mixed-methods approach by combining qualitative and quantitative strategies in the research and narrowing the findings (Hossain & Dwivedi, 2014). Pawlowski and Jung (2015) applied a mixed-methods approach for understanding instructors' selection of strategies through the quantification of students' perceptions of cybersecurity and cybersecurity threats. The student perception variables obtained through qualitative surveys and interviews were manipulated using statistics (Pawlowski & Jung, 2015). A mixed-methods approach is appropriate when qualifying relevant variables and then quantifying the research interpretations of those variables (Trafimow, 2014). My goal was to qualify business leaders' strategy selections in data protection to reduce data loss from cyberattacks without quantifying my interpretations. The quantitative and mixed methods were not fitting to this study as I did not quantify or limit my findings. Quantitative and mixed-methods research were not implemented for this study.

### **Research Design**

A single case study design was applied to the conduct of this study. Green et al. (2015) recommended a single case study design for conceptual models when the case is (a) unique, extreme, or revelatory; (b) representative or typical; and (c) a potential need exists for a longitudinal study. Percy et al. (2015) discoursed the usefulness of a single case study during in-depth investigations when recognizable boundaries are established to differentiate the case from other designs. Baškarada (2014) supported qualitative case study design when there is little information or understanding about the phenomena of interest. I established the case study as a ME defense industry business with worldwide

operations located in Brevard County, Florida. Tsohou, Karyda, Kokolakis, and Kiountouzis (2015) applied information security research to a case study design with a specific public sector organization providing information systems services in Greece. Tsohou et al. investigated *how* and *why* changes occurred with security awareness programs within a selected organization based on organizational, individual, and technological changes. I used the case study design to explore a ME where IS and IT business leaders are successfully applying data protection strategies to reduce data loss resulting from cyberattacks.

Other research designs exist for application with a qualitative approach. Examples of these research designs include ethnography, phenomenology, and narrative study designs. These types of designs offered aspects that were not suitable for use in this study. Ethnographic research is studying a culture of people for a prolonged period (Fusch & Ness, 2015). As my time was limited to weeks or several months versus years, an ethnographic approach was unrealistic. Researchers applying an ethnography design in a qualitative approach seek to define a culture based on the groups' social customs, beliefs, or behaviors observed during the research (Percy et al., 2015). Johnson et al. (2017) suggested an ethnographic approach is informative for understanding decision making associated with a group of people that develop a culture (i.e., emergency medical personnel). I intend to explore *why* and *how* a business leader selects a specific set of data protection strategies to reduce data loss subsequent a cyberattack. My focus contrasts with the ethnographic approach that entails understanding the defense industry business

culture and the influence in business leaders' decision making for protecting corporate data. Ethnography was not an appropriate design for the conduct of this study.

Phenomenology study design was not appropriate for the conduct of this study. A phenomenological design is concerned with the shared experiences of a group of people to determine the similarities in the experiences (Percy et al., 2015). The objective of this study was to gain insight into business leaders' selected data protection strategies that reduce data loss from a cyberattack. I did not seek to understand the problem from the participants' view of their lived experiences in implementing data protection strategies. Fusch and Ness (2015) explained the choice of study design has impacts to data saturation. The phenomenological approach uses a less explicit design for investigating a phenomenon that alters the time till data saturation (Fusch & Ness, 2015). Phenomenology is focused on the essence of the cognitive aspects of the group of people sharing the experience (Percy et al., 2015). Due to limited resources with time and money, a phenomenological study remained unrealistic. I did not seek to understand what a business leader feels like when applying a selected set of data protection strategies nor did I evaluate a group of business leaders for the choices they make in selecting data protection strategies. A phenomenological study was not appropriate for the purposes of my study.

A narrative study was not appropriate for the conduct of this study. Researchers select a narrative approach when focusing on the participants lived experiences through an ordering of events to find meaning among the shared experiences (Singh, Corner, & Pavlovich, 2015). The uniqueness of a narrative approach is the *when* associated with the

*why* (Singh et al., 2015). My focus on this study was *why* and *how* business leaders select the data protection strategies to reduce data loss. I was not interested in when the specific strategies were selected or the experiences of the business leaders leading up to the *when* for the strategy selection. A narrative approach is applicable when a researcher seeks to document and understand a specific event in participants' lives. Bombak and Hanson (2016) used a narrative view to present the meaning of osteoporosis for patients, the lived experience of the osteoporosis diagnosis, and the effects of the osteoporosis prevention and treatment approaches on the patient experience. I did not relate my research on data protection strategies used in reducing data loss to the lived experiences of the business leaders, or how their lives changed after implementation of the selected strategies, nor the effects of the data protection strategies use from the perspective of the business leader. The narrative scholarship also involves the studying of stories to gain insight, capture solutions to problems, note acceptance or rejection of practice, or communicate success and difficulties (Barbour, 2017). I did not seek to gather the stories of ME business leaders related to the problem of data loss. I focused my research on the *why* or *how* business leaders selected data protection strategies to reduce data loss from cyberattacks. Narrative design was not suitable for my study.

Data adequacy and appropriateness support data saturation in qualitative case studies. Tran, Porchar, Tran, and Ravaud (2017) defined data saturation as a point in which new participants no longer change the understanding of the phenomenon. Safarzadeh, Shafipour, and Salar (2018) remarked on data saturation being facilitated by the use of content analysis with semistructured interviews, documents, and observations

to systematically classify the development of codes and themes. Safarzadeh et al. noted that when no additional codes or themes are extracted a researcher achieves data saturation. Morse (2015) bounded data saturation to scope and replication. My data collection consisted of semistructured interviews, review of archival documents, and chronicling my observations. I ensured data saturation based on several factors related to my data collection. The use of purposeful sampling yielded appropriate data based on the selected participants' knowledge and experience relevancy to data protection strategies. The use of these experts restricted and limited the development of themes for rich data. The use of content analysis of the themes developed from the interviews as well as the documents and observations facilitated exploration of the depth of the topic. Fusch and Ness (2015) discussed how data saturation is reached once there is stable integration of themes from the multiple sets of data collected through replication. Data saturation was considered obtained after no new themes were discovered. Research design is foundational to determining population and sampling.

## **Population and Sampling**

### **Defining a Population**

Business leaders that successfully use data protection strategies and reduce data loss from cyberattacks comprised the scope of this case study. Baškarada (2014) described a case study as defined by the unit of analysis (i.e., an event or an organization). The unit of analysis for this single case study was an organization. The organization comprised a single ME located in Brevard County, Florida with worldwide operations. The Small Business Administration (2017) quantified a ME business as an



entity with greater than 500 personnel but less than 2,000 personnel and with annual revenue, not profit, between 10 million and 1 billion dollars. Based on the parameters established by the Small Business Administration, the selected ME consisted of greater than 500 personnel but less than 2,000 personnel and with annual revenue, not profit, between 10 million and 1 billion dollars.

The ME comprised the population for this study employing business leaders within the IS and IT division. A targeted population in a study varies dependent on the focus, purpose, and conceptual foundations of the study but narrow enough to support the research question (Boddy, 2016; Fusch & Ness, 2015; Ngulube, 2015). Palinkas et al. (2015) discussed criteria sampling as a type of purposive sampling used when a researcher knows a group of individuals possess knowledge and experience associated with a phenomenon. In my line of work and my geographical region, I possessed the knowledge of businesses that are small, medium, or large and operating within the different industries (i.e., defense, educational, etc.). I gained insight into the companies that experienced data loss through government contractually driven reporting requirements to my agency. I used further criteria for distinguishing a targeted population from the ME IS/IT business leaders by selecting those IS/IT business leaders only in the decision chain for implementing IT infrastructure and protection of organizational data.

### **Sampling**

I used purposive sampling with predetermined criteria in this single case study and selected five IS/IT ME business leaders. I made the selection from the targeted population of IS/IT business leaders in the ME IT decision chain. Gentles, Charles,

Ploeg, and McKibbon (2015) defined sampling in broad terms as the process of selecting data sources for data collection in support of a research objective. Gentles et al. explained a researcher must communicate the sampling method in the context of said study to lessen ambiguities, increase clarity, and support rigor. The use of purposive sampling aligns with a case study design to meet the research objective in collecting the most relevant data (Baškarada, 2014). Vasileiou, Barnett, Thorpe, and Young (2018) caveated the importance of purposive sampling to provide rich descriptions of data relevant to the phenomenon being studied. The purposive sample of five IS/IT ME business leaders in the decision chain with successful application of data protection strategies aligned with the purpose of the study.

Palinkas et al. (2015) noted purposive sampling as the recognition of information-rich cases for use in research when resources are limited. Barratt, Ferris, and Lenton (2015) acknowledged the benefit of purposive sampling when samples are small. There are additional benefits to purposive sampling with bounding the criteria (Colorafi & Evans, 2016). A smaller sampling strategy enables a researcher to dedicate adequate time to the analysis of a smaller purposive sample size (Fusch & Ness, 2015; Marshall, Cardon, Poddar, & Fontenot, 2013). The use of criteria narrows the sample to those individuals with specific knowledge, expertise, or experience with the problem affording rich data sources (Bengtsson, 2016; Colorafi & Evans, 2016; Fusch & Ness, 2015; Gentles et al., 2015). Palinkas et al. described the use of typical case sampling as suited to researchers learning commonalities and similarities associated with a phenomenon. I used the selected five IS/IT ME business leaders (i.e., those with roles as vice presidents,

department, or team leaders) within the decision chain for IT and IS networks for gaining rich information associated with ME business leaders' successful use of data protection strategies reducing data loss from cyberattacks.

The selected participants participated in semistructured interviews where their expertise in addressing the business problem was shared through their experiences. Using interviews requires consideration of the interview setting. Rimando et al. (2015) explained challenges with the interview environment as related to the researcher, participant, data collection environment, and interview design. Recommendations to minimize these challenges ranged from appropriate dress for the researcher, confidence, and establishing rapport with participants, to participant health, diet, anxiety, room temperature, time of day, or outside weather (Newton, 2017; Rimando et al., 2015). I ensured I dressed in business casual and confirmed this choice of attire was agreeable with the partnering organization and selected participants. The interviewees selected a convenient time and date for the conduct of their interviews. These interviews took place in a setting of the participants choosing and lasted approximately 60 minutes, the length and detail of the participants' responses varied the times. Interviews were semistructured and face-to-face using the interview protocol. I explored the participants' experiences with data protection strategies and used this understanding to address the business problem of data loss resulting from cyberattacks.

### **Ethical Research**

I adhered to specific ethical research requirements, before conducting the research, during the research, and post research inquiry. The *Federal Policy for the*

*Protection of Human Subjects* outlines the appropriate actions to ensure the safety of those individuals participating in research for the benefit of society (Office of the Federal Register, 2017). I conducted this study ethically and adhered to ethical research practices that included the use of informed consent, privacy protections, confidentiality of data, the implementation of a withdrawal process for participants, acknowledgment and receipt of consent to record interviews, securing and encrypting data, and protecting data for 5 years. These practices were conveyed in a participant informed consent form.

I followed an informed consent process to ensure proper disclosure and confidentiality to the partnering organization of study and invited participants. O'Connor, Rowan, Lynch, and Heavin (2017) researched the importance of informed consent to ensure individuals are fully aware of their rights as participants and protection of their data. As part of the informed consent process, I requested approval from the Walden University Institutional Review Board (IRB) through my completion of the IRB application. I provided the final doctoral manuscript and IRB approval number with the publication of my completed study findings. Walden University's IRB approval number for this single case study is 02-25-19-0076587. Bartolini and Siry (2016) discussed in detail the implications of an individual giving consent as the consenting individual's understanding and acceptance of the requestor's needs and the subordination of the individual's own needs to the requestor. I ensured the selected organization and participants understood the consent process to meet the defining characteristics of consent with a written informed consent form. I reviewed the informed consent form with the interview protocol verbally prior to the participant's acceptance for participation in

my study. Informed consent is an active, conscious decision that the participant understands their role in the research (Bartolini & Siry, 2016). I informed selected participants as part of the informed consent that their participation was: (a) strictly voluntary with no paid incentives offered, (b) withdrawing was acceptable at any time for any reason without penalty, (c) incentives were not provided or used, (d) confidentiality was practiced through de-identification of the organization and participants, and (e) data provided by the organization or participants was secured, password protected, and retained for 5 years in adherence to IRB standards and the rights of the participants.

The withdrawal process was the right of the organization or individual participants to withdraw through any means to include verbal or written communication. The partnering organization or selected participants were able to notify me verbally via in person face-to-face, email, or telephone communication regarding their option to withdraw from this qualitative case study. The partnering organization or selected persons were able to notify me in writing at any time of their withdrawal via email or handwritten correspondence. All notifications were to be recorded in my journaling document and retained with the study data however, none were received.

Confidentiality was practiced through de-identifying of the partnering organization and selected persons, by limiting the discussions surrounding collected data, by safeguarding physical data, and digital data. De-identification of the partnering organization and selected persons consisted of everyone receiving an alphanumeric code. The organization was de-identified by the labels of *partnering organization* or *ME with worldwide operations in Brevard County, Florida*. I only discussed the collected data,

when necessary, for the advancement of the data analysis with those Walden University faculty having a need to know. All physical and digital data was safeguarded with a lock box or password protected as appropriate. I used these practices to ensure the privacy of the study participants and the organization.

Data privacy is a crucial aspect of confidentiality and ethics in research. A gap exists between researchers and participants concerning the nature of the information provided by the participant that becomes the researcher's data (Pickering & Kara, 2017; Rimando et al., 2015). A researcher diminishes the gap through early identification of the research objectives (Pickering & Kara, 2017). I ensured the participants understood the objective of my research early in the process by incorporating a restatement of my research objective as part of my written informed consent form and interview protocol. Shordike et al. (2017) spent a week organizing and designing their research and data collection to ensure integration of ethical research practices early in the process. Another aspect of data privacy is the protection of the data.

I protected digital files using an external USB drive with extreme password protection. The USB drive was maintained in a locked container accessed only by me. The audio data files were downloaded from the audio device and retained as digital files protected in the method described above. The physical files were scanned to digital files for back up and protected in the method described above. Any remaining physical data was retained in the locked container as described in the participant informed consent form.

### **Data Collection Instruments**

I used multiple data collection instruments for the conduct of this study. I functioned as the primary data collection instrument. A researcher, as the primary data collection instrument, uses data collected from natural settings for analysis of a phenomenon and development of an understanding from those involved in the study (Peredaryenko & Krauss, 2013). A researcher's health and well-being are another important aspect of the researcher as the primary data collection instrument (Peredaryenko & Krauss, 2013). I attempted to schedule interviews on different days to allow time between the interview and reflexivity of each data collection experience. Peredaryenko and Krauss (2013) acknowledged reflexivity enables the researcher to limit confusion, interpret each data collection experience individually, and minimize researcher fatigue. Subtleties and nuances related to the interviewing tend to be relived through transcription and journaling (Peredaryenko & Krauss, 2013). I used the time in between the interviews to transcribe the interviews and journal my observations.

I used semistructured interviews as a primary data collection instrument. Chu and Ke (2017) characterized semistructured interviews as a pre-determined list of questions supplemented with follow-up questions asked by a researcher when the interview is conducted. A semistructured interview approach also provides some flexibility but through a controlled delivery using an interview protocol (Chu & Ke, 2017; Peredaryenko & Krauss, 2013). I used the semistructured protocol I developed and asked follow-up questions where inquiry served to increase my understanding of information supplied by the participant. Castillo-Montoya (2016) wrote the importance of the

interview as an instrument of inquiry to confirm the purpose and focus of a study. The interview setting facilitates the development of an inquiry-based conversation (Castillo-Montoya, 2016; Peredaryenko & Krauss, 2013; Newton, 2017; Rimando et al., 2015). I used semistructured interviews with the data protection strategy-centric questions listed in the interview protocol as a guide to explore the strategies IS/IT ME business leaders use to improve data protection reducing data loss from cyberattacks.

Secondary data collection instruments consisted of documents (i.e., facility archival documents, security audits, policy, and procedural documents) and journaling (i.e., my informal observations) using the observation and journaling protocols (see Appendices D & E). This type of data collection provides a foundation for naturalistic inquiry and discovery of participant experiences (Colorafi & Evans, 2016). I used documents and journaling to further enrich the qualitative discovery within the study.

I enhanced credibility, reliability, and validity of these data collection instruments through methodological triangulation and member checking. A researcher improves credibility, dependability, and confirmability of their findings using a multi-faceted research approach (Johnson et al., 2017; Yin, 2014). Colorafi and Evans (2016) discussed the importance of using various data collection methods to increase the dependability of the data. Researchers use triangulation to describe various characteristics of a sample population (Colorafi & Evans, 2016). Member checking is a means of ensuring truth in the data and that data make sense to lend credibility to the research (Colorafi & Evans, 2016). I used methodological triangulation of the transcribed interviews, with the results of the content review of the archival documents, and my journaling of the research



process, steps, and observations to maximize the reporting of consistent research findings. I sent each participant the member checking letter (see Appendix B) to use the expertise of the participants to check my analysis of their respective interviews. The methodological triangulation and member checking improved the credibility of my findings, research validity, and increased reliability through reducing bias.

### **Data Collection Technique**

The data collection technique consisted of multiple data collection instruments to include interviews, reviewing archival documents, and journaling through a three-stage process. I pursued data collection only after I received IRB approval. The first stage involved the use of semistructured interviews of the selected sample of participants. Johnson et al. (2017) used semistructured interviews with a small group of ambulance service staff to gain insight into a medical organization and leadership roles. I used semistructured interviews for insight into the data protection strategies to understand how the selected organization reduces data loss from cyberattacks. I developed a participant informed consent form with an interview protocol that met face-to-face with the selected participants to obtain their initial concurrence to participate in the study through a verbal confirmation and then obtained signed consent forms. The informed written consent form included the participation as voluntary, the withdrawal process as flexible and available at any point, the fact incentives were not used, the safety of the participant, and confidentiality with restrictions on information disclosure to include the protection of personal privacy and proprietary information. The interview protocol was used as a guide to conduct the semistructured interviews. I asked each participant the same set of open-

ended interview questions as listed within the interview protocol. Demonstrating consistency with participants ensures integrity and rigor with the data (Colorafi & Evans, 2016; Peredaryenko & Krauss, 2013).

The plan for each interview session was to follow the interview protocol. The interview was intended to last 60 minutes or less given the length and detail of each participant's responses. Shortened time frames limit inconvenience to the participant and the potential for researcher fatigue (Peredaryenko & Krauss, 2013). I afforded the participant the choice of their preferred interview location, date, and time. The location of the interviews may impact participants' responses if the environment is associated with negative influences (Newton, 2017; Rimando et al., 2015). I recorded the interviews using an Olympus digital voice micro-recorder DM620. I transcribed the recorded interviews by hand into a Microsoft word document for storage. Researchers recording interviews increase the avoidance of high inference (Colorafi & Evans, 2016). I developed themes and codes from the transcribed interviews to explore the participants experiences with data protection strategies used to reduce data loss from cyberattacks.

I supported confidentiality using de-identification. Kelly, Branham, and Decker (2016) used semistructured qualitative interviews to research children participating in combat situations. Kelly et al. used a process of de-identification with providing only demographics of the children. Examples of demographics include age, skills, or a role in the community. I de-identified participants based on demographics of years of experience and role in the decision chain. In furtherance of de-identification, I assigned a pre-determined alphanumeric label for the interviewees and removed any additional

identification of their place of business. Researchers make choices about the data obtained in order to best present their findings authentically (Pickering & Kara, 2017). I replayed the recordings to minimize holes and unreliability with the information collected. After I verified the recorded interviews for accuracy, I removed repetitive words and conversation fillers from the manually transcribed interviews.

A final aspect of the first phase was the use of member checking. Morse (2015) used member checking to confirm and correct interview data to support data adequacy and appropriateness. I provided each interviewee a copy of the analysis developed from their interview responses for member checking using the member checking letter (see Appendix B). Once I received the member checking documents from each participant, these were imported into the coding software package (e.g., NVivo). I analyzed these data artifacts, developed from the analysis of the interview responses, for themes and developed thematic codes.

The second phase of my data collection technique included the review of archival documents. I strengthened my interview data with a review of archival documents that included meeting minutes, press commitments, policy, procedure manuals, information systems security audits, and various security reports. These types of documents provided insight into the decision methodologies employed by the IS and IT leaders (Perkmann & Schildt, 2015). A significant aspect of using ANT as a conceptual framework is the layers of networks (Jackson, 2015). The documents served as another layer of the network of interactions between human and nonhuman with regards to data protection strategies employed to reduce data loss. Each document was recorded in my research journal with

document title, date (if present), and type of document. These documents were imported into the coding software package (e.g., NVivo). The archival documents were analyzed for themes and developed into thematic codes.

The final stage of data collection technique involved evaluating my research notes. Peredaryenko and Krauss (2013) substantiated the use of journaling as an important part of the research method by capturing self-reflection. Journaling is a technique to gather data associated with the researchers experience that leads to deductive coding (Chu & Ke, 2017). I journaled the data collection process using observation and journaling protocols (see Appendices D & E) and imported this information into the coding software package as researcher field notes (e.g., NVivo).

There are advantages and disadvantages to the various data collection techniques. Johnson et al. (2017) provided several advantages and disadvantages with data collection techniques that impact qualitative research. The data collection technique of interviewing is straightforward to organize and implement but limitations exist with participants recall of experiences or honesty in their answers (Johnson et al., 2017). Archival document review is a great means for another source of data but is time intensive to review and analyze (Johnson et al., 2017). Journaling is a technique to support triangulation, improve recall, and question or validate other data sources but it is time intensive for the researcher (Johnson et al., 2017).

### **Data Organization Technique**

Organization of the data is important to ensure the integrity and reliability of the study. Data was stored for 5 years after the completion of the study on a USB drive. The

USB drive was maintained in a locked safe to which only the researcher had a key. All data was destroyed through appropriate avenues for digital storage devices 5 years after the completion of the study.

With data organization, privacy and confidentiality are important aspects to maintain in the conduct of this study. All records of participation were kept strictly confidential, such that only the researcher, the committee chair, and those Walden University faculty or peers with a need-to-know had access to the information. The results of the study were reported in a written research study for publication. All identifying characteristics of participants and the participant's employer were kept confidential.

### **Data Analysis**

Yin (2014) described data analysis as a process of critical thinking in the search for patterns, insights, or concepts within the data collected. I used computer-assisted tools for thematic analysis and an analytic strategy to explore and understand the interview data, archival documents, and journaled observations. A recommended approach in developing an analytic strategy entails using case description for analysis (Yin, 2014). A unique aspect of the ANT is the graphical syntax tool that may be used to describe the data in terms of actors and actants to understand the complexity of data protection strategies (Silvis & Alexander, 2014). Park, Shon, Kwon, Yoon, and Kwon (2017) discussed the importance of evaluating themes in research to identify core aspects of a phenomenon. Park et al. used interviews and archived essays of medical students to reveal aspects of professionalism. Xu and Storr (2012) remarked on the importance of

transcription as part of ethics of representation of qualitative research. A researcher must manage the data into identifiable patterns to discern significance of the data (Xu & Storr, 2012). I used thematic analysis and case description to investigate aspects of data protection strategies in reducing data loss from cyberattacks.

I used methodological triangulation to analyze the various data collected. Researchers improve construct validity through analyzing multiple sources of data obtained from different measures of the same phenomenon (Baškarada, 2014). I used methodological triangulation to unite the various data sources into a comprehensive understanding of the data protection strategies business leaders use to reduce data loss from cyberattacks.

NVivo is a qualitative software analysis tool used in qualitative research for the coding of data and themes (Freitas et al., 2017). The use of a qualitative software analysis tool simplifies the interpretation of the research data as well as the writing (Sapat, Schwartz, Esnard, & Sewordor, 2017). Freitas et al. (2017) discussed the efficiencies of using NVivo to organize, explore, and analyze qualitative data. Freitas et al. found the use of qualitative software analysis facilitated a researcher's familiarity with their data and indirectly assisted the researcher's defense of their findings. NVivo is provided free of charge to Walden University students and improves credibility and methodological rigor (Freitas et al., 2017). Salmona and Kaczynski (2016) recommended that early familiarity with the qualitative software analysis tool assists a researcher mastering the benefits of the software. I used NVivo early in my doctoral journey for smaller scoped research studies to increase my familiarity using a qualitative software analysis tool. I

used the qualitative software analysis tool NVivo to code and analyze the themes generated from the data collected.

I used member checking as a final aspect of the data analysis strategy. Member checking offers a means for researchers to advance the understanding, dependability, credibility, and trustworthiness of data (Amankwaa, 2016; Colorafi & Evans, 2016; Johnson et al., 2017; Yin, 2014). I discussed with the participants prior to their interview my use of member checking. I explained how member checking requires their review of my data interpretation and analysis from the recorded interview session. I requested their concurrence of the analysis within a specified period of 5 business days. I also afforded them the option to provide questions, concerns, or additional input on the interview analysis with an email to me during the same time period. If the participant selected to provide input I responded with a revision and ask for concurrence of the revised input within 2 business days. A lack of response from the participant denoted acceptance of the data interpretation and analysis.

## **Reliability and Validity**

### **Reliability**

I used methodological triangulation and member checking to evaluate the data obtained from interviews, archival documents, and journaling. Posner (2016) quantified reliability as an iterative process based on constant application of the instrument with the equivalent results. A yield of equivalent results from methodological triangulation of the data obtained ensures credibility of my data. Bengtsson (2016) noted the interaction between researchers and study participants informs the study results. I used the

participants' expertise and knowledge to check my accuracy of data interpretation and analysis with member checking. These checks and balances enhanced *the dependability* and advanced the reliability of my research.

Bengtsson (2016) noted there is risk with these approaches due to the delay between analyses and confirmation of the researcher's interpretation and analyses. I ensured that methodological triangulation and member checking analyses occurred immediately following each interview. To facilitate this process, I conducted my review of archival documents prior to the scheduling of the interviews; I attempted a minimum of 2 days of separation in between each interview to allow for the analysis of the interviews with the other data sources. Following the process helped ensure I mitigated researcher fatigue. Peredaryenko and Krauss (2013) investigated concerns with researcher fatigue and the impact to the collected data.

I used journaling as part of the methodological triangulation. A researcher journaling the observations during a study has improved the richness of data (Amankwaa, 2016; Neusar, 2014; Peredaryenko & Krauss, 2013). Peredaryenko and Krauss (2013) underscored the importance of journaling to capturing data while it remains fresh in a researcher's mind. I journaled to ensure my interpretations were dependable and accurate. Baškarada (2014) emphasized the use of different measures that arrive at the same results lends to increased validity in research. I used journaling with the observation and journaling protocols (see Appendices D & E) in conjunction with methodological triangulation and member checking to ensure reliability but also support the validity of my research.



## **Validity**

Posner (2016) noted validity is determined based on the intended measure by the instrument. *Credibility* is the confirmation of the collected data by an informant (Bengtsson, 2016). I used my participants, experts in the field of data protection strategies to reduce data loss from cyberattacks, to judge the quality of my data interpretations and analysis. A researcher cannot transfer the applicability of their study findings to that of another study to ensure *transferability* (Bengtsson, 2016). I used descriptions of my research context for this study to enhance the potential transferability of my findings. *Confirmability* relates to the presentation of the data (Amankwaa, 2016; Bengtsson, 2016). Graneheim et al. (2017) discussed authenticity in the data associated with detailing the logic used in presenting the theme selection and interpretation of the data related to the phenomena. Again, journaling my observations through the study lends to the confirmability and authenticity of the data presented. *Data saturation* is the point in which a researcher obtains no further new information, coding, themes, and the replication of results is achievable (Fusch & Ness, 2015). I used a small purposeful sample of experts with semistructured interviews and member checking to ensure the scope of the study is narrow enough to obtain rich data.

## **Transition and Summary**

Cybersecurity involves the protection of data. Business leaders must evolve data protection strategies to defend against the pervasiveness of cyberattacks (Cook, 2017). This qualitative study was focused on understanding the data protection strategies used by a single organization to successfully protect against data loss from cyberattacks. In

Section 2, I detailed a review of the purpose and problem of data protection to reduce data loss from cyberattacks. As the sole researcher for this study, my participant selection requirements for the study population and sampling were outlined. I presented my research design and methodological approach. I discussed the ethics of my research to ensure compliance with ethical standards. I provided a basis for data collection including the instruments, techniques, organization, and analysis of the data ensuring the mitigation of potential risks to the data collection process. Section 2 was closed with a discussion of the reliability and validity of the data. I identified the criteria behind the selected qualitative methods I used in this study. The use of these qualitative methods was helpful to ensure the dependability, creditability, transferability, and confirmability of the data.

Section 3 is a presentation of the findings from the conduct of this qualitative single case study. In the section, I will provide application to professional practice, implications for social change, recommendations for action and further research. I will offer reflections on my experiences with the doctoral study process. Lastly, I will close with concluding statements and an informative message regarding data protection strategies to reduce data loss from cyberattacks.

### Section 3: Application to Professional Practice and Implications for Change

#### **Introduction**

The purpose of this qualitative, single case study was to explore the strategies ME business leaders use to improve data protection to reduce data loss from cyberattacks. The targeted population consisted of five ME business leaders in the cleared defense industry who were (a) part of a ME with worldwide operations in Brevard County, Florida; (b) part of the IS/IT decision chain for implementing data protection strategies; and (c) possessed a bachelor or higher education degree in business or information management, or possessed a minimum of 3 years working experience in an IS/IT related discipline for a department of defense contractor, and 1 year or greater working specifically with protecting data. The conceptual framework for this study was the ANT. I informed the research question using the partnering ME organization archival documentation, semistructured interviews with open-ended questions and subsequent responses, and my research journaling. The overarching major theme categories developed from the data analyses are *people* inferring security personnel, network engineers, system engineers, and qualified personnel to know how to monitor data; *processes* inferring the activities required to protect data from data loss; and *technology* inferring scientific knowledge used by people to protect data from data loss. I analyzed the research findings and determined the effective strategies for improving data protection to reduce data loss from cyberattacks.

## Presentation of the Findings

The research question for this study was “What strategies do ME business leaders use to improve data protection to reduce data loss resulting from cyberattacks?” I identified major and minor themes using thematic analysis. Figure 1 shows the themes derived from the literature review using a mind map illustration.

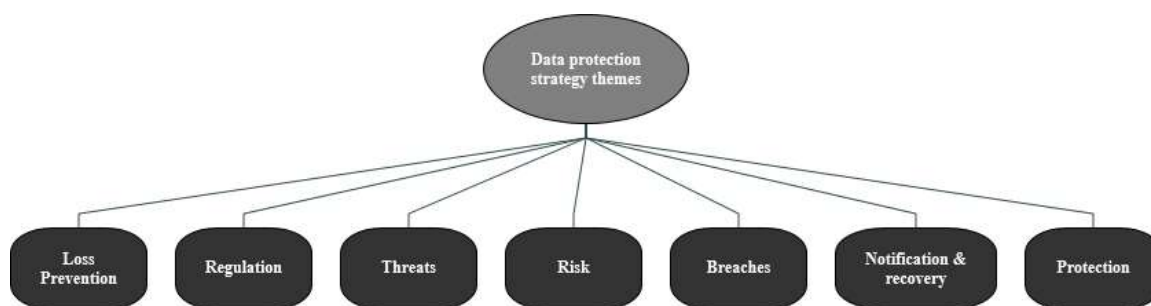


Figure 1. Data protection strategies mind map of themes from literature review.

In relation to these themes, my analysis and findings indicated that *people* (i.e., security personnel, network engineers, system engineers, and qualified personnel to know how to monitor data); *processes* (i.e., the activities required to protect data from data loss); and *technology* (i.e., scientific knowledge used by people to protect data from data loss) are critical to data protection and preventing or mitigating data loss resulting from cyberattacks. Determining a balance between these aspects with the goal of securing BCI while sustaining successful business operations is a challenge for ME business leaders. Minor challenges involve hiring the right experts, supporting the experts with policies, defining processes supporting data protection, and implementing appropriately configured and deployed technology. Additional challenges exist with security education awareness and training for IS/IT security professionals and end users of the network systems. Another key challenge my analysis and findings revealed is the need for ME

business leaders to understand their own data, where it physically resides on their system architectures, the mobility of the data, and how to best secure the data.

I used NVivo data analysis software to analyze the member-checked interviews, company archival documents, and journaling notes (i.e., field notes). I referred to each IS/IT business leader as a participant in this study with the letter P and a number (e.g., P1, P2, P3, P4, and P5). Thematic analysis occurs in two levels: semantic, which results from a surface meaning of the interpreted data, and latent, which results from the interpretation of the underlying ideologies that inform the semantic content (Maguire & Delahunt, 2017). There are multiple different techniques for theme identification (Ryan & Bernard, 2003). I chose to apply theory related material that characterizes the experience of the participants combined with word lists and key words in context.

I used a multi-level approach to the coding and theming based on the work of Maguire and Delahunt (2017). I coded and thematized within each data collection group (i.e., member-checked interviews were coded and themed, researcher field notes were coded and themed, etc.), obtaining surface (i.e., semantic) meanings of the related themes. Then, I coded and themed the collective group of data artifacts incorporating triangulation and discerning the latent themes from this level of analysis. In this section, I provide a discussion of the triangulated themes in terms of confirming, disconfirming, or expanding the themes presented in the literature review. Additional new literature with evidence from this study were presented to support the discussion of my findings. This approach to the analysis ensured that I achieved data saturation by using all data collected with integrating member checking and methodological triangulation. This

compartmentalized approach was important in simplifying, condensing, and interpreting the various themes into the overarching theme categories.

### **Member-Checked Interviews Themes**

The member-checked interviews resulted in four major themes: (a) threats, (b) network, (c) security, and (d) data. The member-checked interviews led to six minor themes: (a) tools, (b) strategies, (c) people, (d) key challenges, (e) access, and (f) users. Table 1 is a display of the frequency of member-checked interviews themes for this study. The results indicate that the participants viewed strategies in terms of the threats to the data, the network where the data exists, the security used to protect the data, and the data itself in terms of classifying the data.

Table 1

#### *Frequency of Member-Checked Interview Themes*

Themes	<i>N</i>	Frequency of code
<b>Threats</b>	<b>30</b>	<b>24%</b>
<b>Network</b>	<b>19</b>	<b>15%</b>
<b>Security</b>	<b>17</b>	<b>13%</b>
<b>Data</b>	<b>14</b>	<b>11%</b>
Tools	9	7%
Strategies	8	6%
People	8	6%
Key challenges	8	6%
Access	8	6%
Users	6	5%

*Notes.* *N* = frequency.

Relevant comments to support the member-checked interviews themes include the following:

With enhanced security using multi-factor authentication, virtual private network, jump servers, user privileged access, auditing, patching, virus software, specific security controls, and encryption to manage who gains access to data on the firm's servers . . . forms a layered approach to protecting data (P1).

This strategy [least privilege] only allow[s] those users access to the data when justification is provided (P2).

Technical threats is being aware of the vulnerabilities in technologies such as: (a) weak protocols, (b) unsecure transfer of things, (c) plaintext of protocols, and (d) malicious suites (P3).

Applying the strategies to ensure that the correct users receive the correct permissions with respect to the data and that you apply the tools . . . the correct way (P4).

Top level architecture which is a method of layering your information security into an approach understood as security in depth. [Using] International Standards Organization open systems interconnection model . . . divides the connectivity of the network into layers where the lower layers deal with connectivity between the data movement and the upper layers deal with applications of and for data use (P5).

Figure 2 illustrates the frequent words appearing in the member-checked interviews. Analyzing the themes from the member-checked interviews word frequency indicated the importance participants placed on the data in designing the appropriate data protection strategies. More importantly, the visual captures supporting words such as

security, network, architecture, system, access, layers, movement, protection, threat, software, and firewalls.



*Figure 2.* Word frequency query results for member-checked interviews.

### **Researcher Field Notes Themes**

Table 2 displays the frequency of my field note themes for this study. The results indicated a reflection of the major themes as (a) data, (b) network system, and (c) threats as critical in my observations of the phenomenon of data protection strategies. I noted the minor themes from my observations as (a) access, (b) tools, (c) training, (d) users, (e) data protection, (f) key challenges, (g) security, and (h) management. I observed the participants' perspectives of data protection strategies as associated with the firm's data, network systems, and threats against the firm's data.



Table 2

*Frequency of Researcher Field Notes Themes*

Theme	<i>N</i>	Frequency of code
<b>Data</b>	<b>28</b>	<b>20%</b>
<b>Network system</b>	<b>18</b>	<b>13%</b>
<b>Threats</b>	<b>17</b>	<b>12%</b>
Access	14	10%
Tools	14	10%
Training	12	9%
Users	11	8%
Data protection	10	7%
Key challenges	9	6%
Security	7	5%
Management	1	< 1%

*Notes.* *N* = frequency; < is greater than.

The results indicated a reflection on the data protection strategies in terms of the data, the network system where the data exists, and the threats to the data. Selected comments supporting these field notes include:

- P1 noted that zero day threats, phishing attempts, and e-mails were some examples of technical threats to the firm's data that influenced the selection of next generation virus software, third-party e-mail filtering to improve analysis of the threats, patch management, backup systems, e-mail-based data protection tools such as a phishing button, and security training and awareness strategies to improve data protection to reduce data loss resulting from cyberattacks.
- P2 found that data protection strategies such as default denials of access and implementing business cases where access requests to the data are defined

establishes a framework to determine access to the data that works best to improve data protection to reduce data loss from cyberattacks.

- P3 noted vulnerabilities resulting from the reliance on technology and failure to understand the tool suites in relationship to Internet penetration points as technical threats to the firm's data that influenced the selection of data protection strategies.
- P4 noted insider threats from disgruntled or terminating employees as the key influencer for selection of strategies such as using software tool suites to detect or trigger a DLP.
- P5 contributed the following additional information: the need to minimize a false sense of security in technology and investing money in technology without training or understanding the technology creating redundancy without protecting the data, vetting the personnel to ensure expertise, implementing logical data protection strategies to compliment the firm's work, ensuring that monitoring, patching, and auditing are taking place, and vetting third-party vendors.

Figure 3 shows the frequent words appearing in my field notes. The analysis of the word frequency indicated the importance I placed on data in determining the appropriate data protection strategies. Figure 3 captures supporting words such as threats, training, protection, strategies, security, network, protection, access, firm, understanding, tool, phishing, access, challenges, awareness, and users.



*Figure 3.* Word frequency query results for researcher field notes.

### **Archival Documents Themes**

The archival documents are differentiated into three groups: (a) plan documents, (b) policy documents, and (c) standards and applications documents. The purpose of a plan document is to provide the overarching processes and procedures to support the decisions and actions used for adherence to policies. The policy documents afford clarification and instruction on how the firm is to meet a requirement, regulation, or deal with accountability (i.e., government, industry, or legal specific). Policy documents are in place to ensure the company personnel operate in terms of what is critically important to the business. The purpose of the standards and applications documents is to provide a benchmark for facilitation of communication, measurement, and tools when implementing company plans to meet a requirement, regulation, or accountability.

Table 3 displays the frequency of archival documents themes for this study. The thematic analysis of archival documents yielded three major themes: (a) system, (b) information, and (c) information systems. There were also 13 minor themes: (a) security,

(b) user, (c) company, (d) access, (e) business, (f) e-mail, (h) accounts, (i) network, (j) data, (k) software, (l) messages, (m) addresses, and (n) personal e-mail. The results of the archival documents themes are an indication of the partnering organization's emphasis on the systems, information, and information systems when developing the plans, policy, standards, and applications to support chosen data protection strategies.

Table 3

*Frequency of Archival Documents Themes*

Theme	<i>N</i>	Frequency of code
<b>System</b>	<b>238</b>	<b>20%</b>
<b>Information</b>	<b>203</b>	<b>17%</b>
<b>Information system</b>	<b>129</b>	<b>11%</b>
Security	96	8%
User	93	8%
Company	86	7%
Access	67	6%
Business	52	4%
E-mail	42	4%
Accounts	39	3%
Network	35	3%
Data	32	3%
Software	22	2%
Messages	19	2%
Addresses	10	1%
Personal e-mail	8	1%

*Notes.* *N* = frequency.

The frequency of archival documents themes supports the interpretation that the partnering organization's plans, policies, and standards and applications focus on the information systems and IT. This reliance on the enterprise may be an indication why many of the selected strategies are integrated across the business enterprise.

Figure 4 illustrates the frequent words appearing in the archival documents' themes. I analyzed the themes using the word frequency chart and while the themes are an indication of the importance placed on systems, information, and IS, data is in the key focal point in the word frequency chart. The visual reflects the additional words within the archival documents that indicate other focus areas for data protection such as: access, security, company, control, protection, requirements, management, users, business, maintenance, servers, network, and process.



*Figure 4.* Word frequency query results for archival documents.

### **Methodological Triangulation of Coded Themes**

I combined the nodes from the coded data groups developed for member-checked interviews, researcher field notes, and archival documents using the autocoding feature in NVivo as a means of methodological triangulation. Table 4 is a display of the frequency of triangulated themes for this study. The triangulation analysis yielded three major themes: (a) network, (b) security, and (c) people. There were nine minor themes in the findings from triangulation: (a) access, (b) company, (c) data, (d) business, (e) threats, (f)

tools, (h) key challenges, (i) training, and (j) strategies. The results of methodological triangulation are an indication of designing data protection strategies based on enhancing network technologies (i.e., network), impact assessments (i.e., security), and individual privacy (i.e., people).

Table 4

*Frequency of Triangulated Themes*

Theme	<i>N</i>	Frequency of code
<b>Network</b>	<b>760</b>	<b>53%</b>
Security	120	8%
People	119	8%
Access	89	6%
Company	86	6%
Data	84	6%
Business	52	4%
Threats	47	3%
Tools	45	3%
Key challenges	17	1%
Training	12	1%
Strategies	8	1%

*Notes.* *N* = frequency.

The table shows the major and minor themes of the frequency of triangulated themes for this study. Network was the most frequent theme. An indication that most of the data protection is spread through the network, use of network technologies, and supported by policy, plans, standards and applications applied to the network.

Figure 5 is the visual representation of the frequent words appearing in the triangulated data. The most prominent words from methodological triangulation are information, system, and data with supporting word frequencies of access, business, company, and security. The minor word frequencies consist of user, users, management, system, server, control, software, must, maintenance, and requirements.



*Figure 5.* Word frequency query results for triangulated data.

I found in analyzing the triangulated themes there is an ad hoc approach to data regulation, a concentrated focus on and countering potential threat vectors specifically the human threat in terms of the user and insider, consideration of future threat environments, incorporation of risk management, understanding of data breaches as these pertain to the organization, assiduous DLP efforts, inclusion of data breach notification and recovery principles, and data protections in terms of BCI.

**Data regulation and triangulated themes.** My analysis confirmed an ad hoc approach to organizational data regulation. Sarabdeen and Moonesar (2018) concluded that an absence of unified data protection regulation leads to organizations self-regulating. The partnering organization in this study incorporated NIST and International Standards Organization standards as well as benchmarking to proscribe policy, plans, standards, and applications. I noted an overall reliance on best practices in both the interview interpretation and archival document reviews. For example, P1, P3, and P5 noted the use of these ad hoc approaches using NIST, International Standards

Organization, and benchmarking as successful data protection strategies. The plan documents contained references to NIST approved configuration standards and voluntary consensus security configuration standards and benchmarks. Bellanova (2016) posited a finding, based on earlier work of Michel Foucault, French philosopher, that the world is moving towards a governmentality of data-driven governance. My findings support this assumption noting how the themes network, security, and people are used to govern the organization through the protection of their digital data (Bellanova, 2016). In terms of ANT, Lupton (2016) expressed the notion that sociotechnical assemblages created by the network actors (i.e., network, security, and people) is the creation of data as a species (2016). The major triangulated themes of network, security, and people are an example of how firms quantify (i.e., benchmark) the relationships with data protection that lead to governance (Bellanova, 2016; Rose & Miller, 1992). More importantly, Jacobs and Popma (2019) signified ad hoc data regulation design as a data protection strategy that promotes governance by digital data and benefits the subjects of the data protection (i.e., corporations).

**Extending the knowledge concerning data threats.** My analysis extended the research on the data threats and resulting vulnerabilities as persistent and evolving. I interpreted the firm's understanding of BCI complexities in terms of threats and vulnerabilities directly related to the data lifecycle. The data lifecycle as the movement of data, data at rest, and protection of the data as it materializes through controlling of the data (Calvard & Jeske, 2018; Hintze, 2018).



All participants referred to controlling the data lifecycle as defining permissions, limiting privileges and accesses, designing specific connectivity plans, and the use of various tools (i.e., jump serves, VPS, software, passwords, encryption at rest, and demilitarized zones). This evidence was characterized in both the major and minor themes to include network, security, people, access, company, and threats. For example, the themes of access and threats appear in all member-checked interviews and researcher field notes as a nontechnical threat that drives data protection strategy selection (i.e., insider threat). Additionally, the insider threat is a pronounced theme in the archival documents, specifically with how this threat is identified, physically protected against, and the standards to document and control the data in terms of the threat.

In terms of ANT, Tsohou et al. (2015) explained how the relationships between the organization, technologies, and individuals is continually changing, evolving, and drives the development of the interactions between the network, security, and people. In the specific example cited by Tsohou et al. it is information security awareness. The use of information security awareness effectually becomes a means of controlling data to counter threats.

**Findings confirm risk mitigation as a priority.** Lavastre, Gunasekaran, and Spalanzani (2012) and Blome, Schoenherr, and Eckstein (2014) captured the importance of risk mitigation as alignment to business strategies, adherence to regulatory requirements, employee skill sets, vetting vendors and suppliers, preparing for economic impacts, technological, social aspects, infrastructure of IS/IT equipment, and natural disasters. Whitley and Farris (2017) underscored the importance of organizational leaders

and stakeholder's acceptance and support in selection, implementation, and active monitoring of strategies to protect and reduce data loss.

This theme of risk mitigation as a priority is indirectly prominent in the findings of this study. The triangulated data contained multiple references to risk mitigation without specifically identifying risk mitigation as a theme. For example, the major and minor themes of network, security, people, access, company, business, threats, and tools are all required functions to explain or limit the probability of loss and or damage to BCI (Aven, 2016). The participants, archival documents, and my notes contain multiple references to one, some, or all of the requirements for risk mitigation to include: (a) business strategy aligning with securing the data, (b) adherence to regulatory requirements such as NIST, International Standards Organization, and benchmarks; (c) the importance of hiring the right people with the needed skill sets, (d) vetting vendors and suppliers before granting them access to organizational data, (e) preparing for technical and nontechnical threats such as phishing attempts, (f) social engineering, (g) aging of infrastructure or IS/IT equipment, and (h) natural disasters.

The conceptual framework for this study, ANT, was useful in understanding the gaps in risk mitigation regarding the activity of current actors and enlistment of additional actors. Stachel and DeLaHaye (2015) captured the importance of how ANT translates risk mitigation. In an annual benchmark study of patient privacy and data security it was noted that 65% of respondents acknowledged the use of non-secure databases to maintain patient data (Ponemon Institute, 2014). In determining a theory to explain the complexities associated with protected health information (PHI), Stachel and

DeLaHaye demonstrated how ANT is used to determine approaches to risk mitigation. Most notably, the use of ANT is a way to identify needs to increase activity of actors in the network and enlist new actors in the network (Stachel & DeLaHaye, 2015). As applied to this study, P1 and P4 indicated strong activity with organizational leader support and the increased enlistment of third-party vendors for data protection measures. The organizational leader support in terms of funding the use of vendor software and training to enable detection of purged data by a hacker or insider threat by filtering, testing, and analyzing network traffic.

**Extending and confirming data breaches strategies.** The outcomes of the study findings disconfirm parts of the peer-reviewed studies on data breaches from the literature review. In the literature review, it was noted that an underlying cause for data breaches is the business leaders' over-reliance on technology (Layton & Watters, 2014). Another noted cause for data breaches is the lack of security controls and protections (Connolly et al., 2017). I analyzed the triangulated data and affirmed a strong understanding by the business leaders of the data, the connectivity to their data, and the use of technology in understanding how the security controls monitored the movement of data within the firm infrastructure. The major themes of network, security, and people supported this finding with the participants noting the use of software and third-party vendor tool suites with specialized training to monitor and mitigate data breaches. This study is a corroboration of the work of Gwebu et al. (2018) on how a firm's knowledge of available tools prevents data breaches and increases safeguarding of data to minimize data breaches and financial impacts.

**Data loss prevention strategies are confirmed.** The DLP strategies were confirmed with the findings. The analysis of the data demonstrated how the partnering organization used many of the DLP strategies researched in the literature review. Many of the DLP methods used included data categorization, user profiling, and tracking and restricting data access (Arbel, 2015). All participants in some facet addressed one or several of the DLP methods. Another finding confirmed during the analysis is technology, people, and processes create vulnerabilities. Meaning businesses need to consider the context of how insider and outsider threats use people, processes, and technology to gain access to the company data. Participants stated safeguarding data and mitigating loss through network security with constant monitoring and training of personnel are best practices such as password use, personal monitoring and protection personal monitoring (Arlitsch & Edelman, 2014)

**Notification and recovery strategies are confirmed.** The findings for notification strategy was confirmed during analysis. The notification strategy researched in the literature review consisted of monitoring of the data in various stages (i.e., movement and at rest). P1 noted third-party vendors are used for monitoring, auditing, and implementing a layered security approach to monitor the data movement within the system architecture. P2 noted audits must include internal and external auditing. P3 stated security suites, monitoring, auditing, and documenting activity occur in the networks. P4 stated software (i.e., Netrics) is used to monitor and notify [system and network engineers by using alerts of] any changes. P5 noted the use of security protocols to monitor data traffic as import in notification.

The recovery strategy during this study is a confirmation of the literature review. The focus of recovery from data breaches is on the investigation of the data breach (Plachkinova & Maurer, 2018). Also, incorporating external services to assist (e.g., action reports) with improving data security (Gootman, 2016). All participants remarked on the use of implementing least privilege access, third-party vendor tools, and updating processes and policies to support a layered security approach to the network architecture.

**Overall data protection strategies are confirmed.** In understanding the use of overall data protection strategies, ME business leaders must incorporate security awareness and training for their people, a policy infrastructure to support their processes, and standards and applications for maximizing the use of technology to reduce data loss. The fact business leaders must know the value of their data is confirmed with the analyses of this study. Specifically, the use of technical and organizational measures as a function of threats and vulnerabilities to mitigate risk. The participants in their various responses identified data as requiring least permissions, using auditing for the detection of threats, patching to respond to threats, and backing up the system to recover data in the event of a data breach (P1, P2, P3, P4, & P5). P1 specifically noted the use of rigorous controls confirming the protection of the data as a foundational element of BCI, sensitive, proprietary, and PII. NIST security controls and third-party vendor suite tools were identified as the frameworks used by the partnering organization to tailor the security controls based on the organization's data protection requirements (P1 & P5). In terms of the ANT conceptual framework and the overall data protection strategies, the study findings are a confirmation of the work of Thumlert et al. (2015) and Walls (2015). These

findings also extend the work of Hung's (2017) use of ANT in understanding data protection assemblages as translations of assemblages and multiplicities within assemblages (see Figures 7-13). The indications of the findings are that data protection strategies to reduce data loss are innovated ideas. These innovations are developed as an outcome of the stabilized network of interactions between actors and actants in the many heterogenous network assemblages existing within the partnering organization.

### **ANT-gs, Data Protection Strategy, and Reducing Data Loss.**

ANT-gs is a visual method used to showcase how the ANT conceptual framework is used for the development of a data protection strategy, in this case, an architecture security strategy. Key tenets of ANT are problematization, interessement, enrollment, and mobilization (Burga & Rezania, 2017; Jackson, 2015; Silvis & Alexander, 2014). In this example, I showcased how ANT-gs is a visual representation of ANT and these key tenets (Burga & Rezania, 2017). The problematization of architecture security is the initial positioning of the data, external threat, end-user, and data breach actors that establish as an obligatory passage to define the roles and responsibilities of additional actors in solving the issue of architecture security (Mähring et al., 2004).

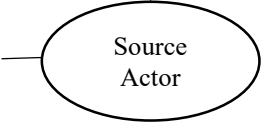
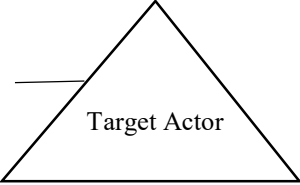
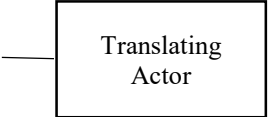


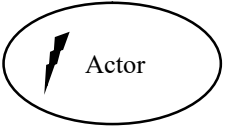

The interessement stage in this example is the alliances implied by business leaders, ideas, processes, technologies, and people that become part of the network (Burga & Rezania, 2017). As each actor formalized into their respective roles and responsibilities the secure architecture enters the enrollment phase of the ANT (Mähring et al., 2004). Translation, the final stage, is the result of efforts between the various actors as assemblages of the network that promulgated the secure architecture into a stabilized

actor-network and inherently a black box (Iyamu & Mgudlwa, 2018; Mähring et al., 2004).

ANT-gs uses various symbols to capture the translations taking place between actors in a network through the stages of ANT. In the example of architecture security strategy (as shown in Table 5), a circle, a triangle, a square, bolded square, a circle with a lightning bolt, and a cloud are used to indicate different translation actions occurring within the network. The circle is an actor within the architecture security network. The triangle is a targeted actor receiving a translation from another actor in the network. The square is a translating actor between a source actor and a target actor. The bolded square is an indication of an established network that is functioning as a source actor, target actor, or a translating actor. The circle with a lightning bolt is symbolizing the existence of an actor that is either physically or conceptually distant from the active network but influencing the network. The final cloud symbol in the architecture security strategy network is symbolizing an actor that may not be within the active network but is not distant physically or conceptually and is not an established, stable network but influences the translations.

Table 5

*Meanings of ANT-gs Symbols*

Concept		Definition	Graphic symbol
Source	Core concept	Any entity that is included in an ANT analysis	
Target	Core concept	Any entity that is included in an ANT analysis	
Translator	Core concept	Any entity that is included in an ANT analysis that translates between a Source and a Target	
Relationships	Core concept	Indicates the relationship between a <i>Source</i> , <i>Translator</i> , and <i>Target</i>	
Black box	Complex ANT concept	A black box is a well-established network of allied actors that is so strong that the assemblage is counted as only one actor	
Actors at a distance	Complex ANT concept	Action at a distance identifies an actor that can act upon another that is far away from itself (physically or conceptually)	
Exemplary instances	Pragmatic extension	Actors that do not explicitly form part of the empirical dataset, but which might nevertheless form part of the actor-network	

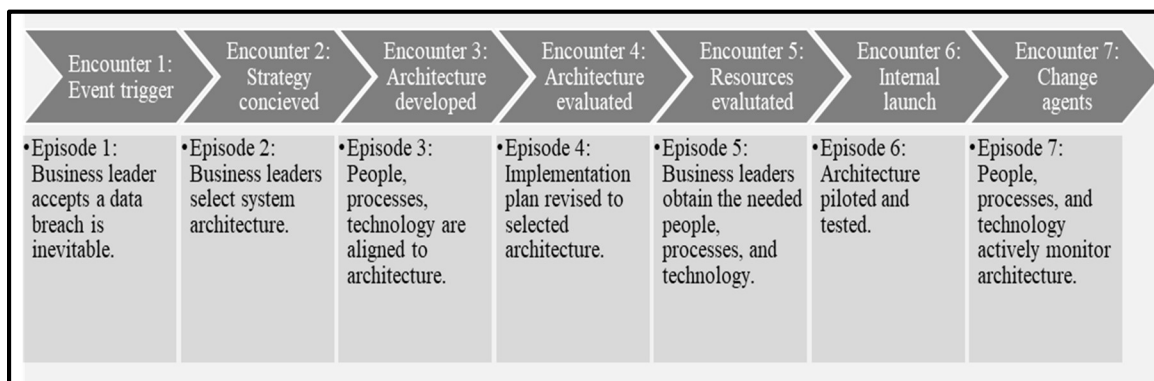
*Note.* Adapted with permissions from "A study using a graphical syntax for actor-network theory," by E. Silvis and P. M. Alexander, 2014, *Information Technology & People*, 27, p.114.



It is useful to understand the symbols that differentiate the actors and their alliances to enable a visual depiction of translations between the actors within the actor-network (Silvis & Alexander, 2014). The circle, triangle, and square are symbols that form the ANT-gs based on concepts associated with the roles that actors can portray in translation (Silvis & Alexander, 2014). The next concept not yet presented is the solid lines representing relationships between the various actors. A relationship may signify an alliance between the actors (Silvis & Alexander, 2014). The bolded square and circle with lightning bolt are depicting complex ANT concepts. The first concept of black boxes (i.e., the bolded square), reflects the existence of a different stable and complex actor-network assemblage (Silvis & Alexander, 2014). The second concept (i.e., the circle with the lightning bolt) is illustrating the actions of one actor physically or conceptually at a distance from another actor (Silvis & Alexander, 2014). The final concept (i.e., the cloud) is for those actors with an influence on the assemblage, acknowledged as part of the assemblage but may have a multiplicity, and may not necessarily have been analyzed in depth (Silvis & Alexander, 2014).

ANT-gs may be used to develop a model for depicting an actor-network assemblage. In my study, I used ANT-gs to depict a data protection model for an architecture security strategy. When constructing a model using ANT-gs, the model is broken down into encounters and episodes over a period (see Silvis & Alexander, 2014). Silvis and Alexander (2014) explained an encounter as an event that challenges an expected path within a process. The episodes are the actions that take place between encounters (Silvis & Alexander, 2014). The data protection model is a tool for

developing other types of data protection strategies. To showcase how this is accomplished I used the data protection model to visually capture the various encounters and episodes of an architecture security strategy that was understood from the semistructured interviews conducted with the IS/IT business leaders in this study. As shown in Figure 6, Encounter 1 reflects an event triggering Episode 1. In this case the event would be the data breach. The episode is the business leader accepting the data breach has occurred or is inevitable. Encounter 2 is the IS/IT business leader walking the current architecture and the environment for the architecture and conceiving the idea of the proposed revised architecture. Episode 2 is the business leader accepts the conceived strategy for the architecture security. Encounter 3 involves the development of the architecture. This leads into Episode 3 where various actors are mobilized through enrollment creating alliances. Encounter 4 is the evaluation of the architecture. Episode 4 is the translation of the evaluated architecture into an implementation plan. Encounter 5 is where the IS/IT business leaders evaluate the implementation plan required resources. Episode 5 is obtaining the require resources such as the people, processes, and technologies. Encounter 6 is the internal launch of the implemented architecture security strategy that leads into Episode 6 that involves piloting and testing. Encounter 7 is the identification of change agents. These change agents in Episode 7 continuously monitor the architecture security.



*Figure 6.* Encounter-episode framework for architecture security strategy data protection model.

The remaining figures (Figure 7-13) are the resulting graphical ANT data protection models using the ANT-gs symbols to depict each encounter-episode framework described above for the architecture security strategy. For example, Figure 8 is the Encounter-Episode 1 with the actors' outside threat, end-user, data breach, and data. The outside threat and end-user actors are both functioning as source actors with data as the target actor and the actions of each is translated by the data breach actor. Each successive figure captures these actions between actors, new target actors, and translations between actors to show how the network takes shape. The final figure (see Figure 13) is the graphical representation of how the network stabilizes as a secure architecture security strategy network. Additional important aspects of the ANT demonstrated in these figures (see Figures 8 through 13) is multiplicities, black boxes, and actors by a distance. In Figure 9, the data owner is a target actor as well as a source and translating actor. In Figure 9, the black box fraud detection is a target actor responding to the data breach first, then a source actor enrolling the data owner, IS/IT engaged, executive management, and security management actors. Then, finally, a

translating actor between the data and the data owner, IS/IT engaged, executive management, and security management actors. Fraud detection is also shown as a black box because it is a stabilized network of interactions of other actors and actants that takes place in order to become a source, target, and translating actor. Meaning, as I have modeled the architecture security strategy in these encounter-episodes, I can model fraud detection strategies using ANT due to the complexities of the actors and actants involved with fraud detection.

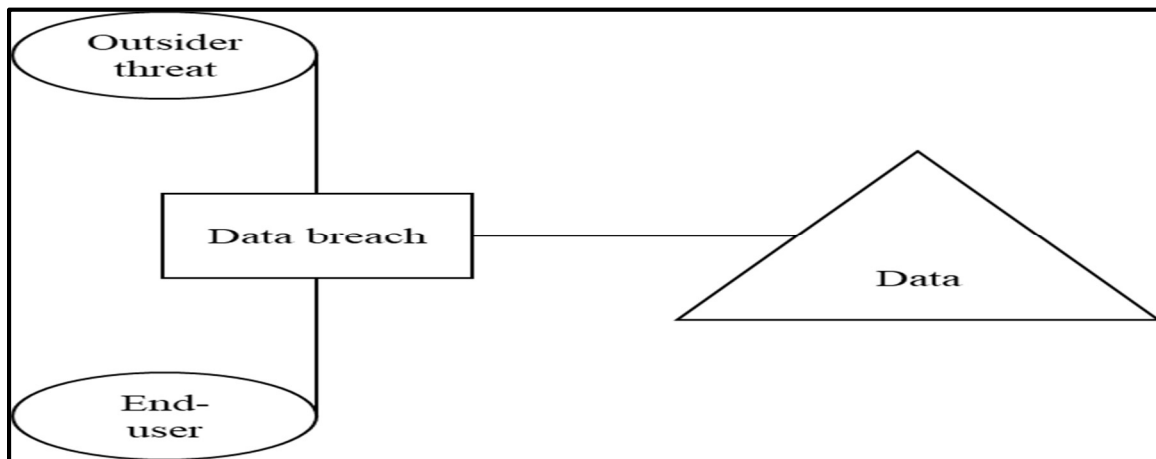


Figure 7. Encounter-episode 1 of architecture security strategy.

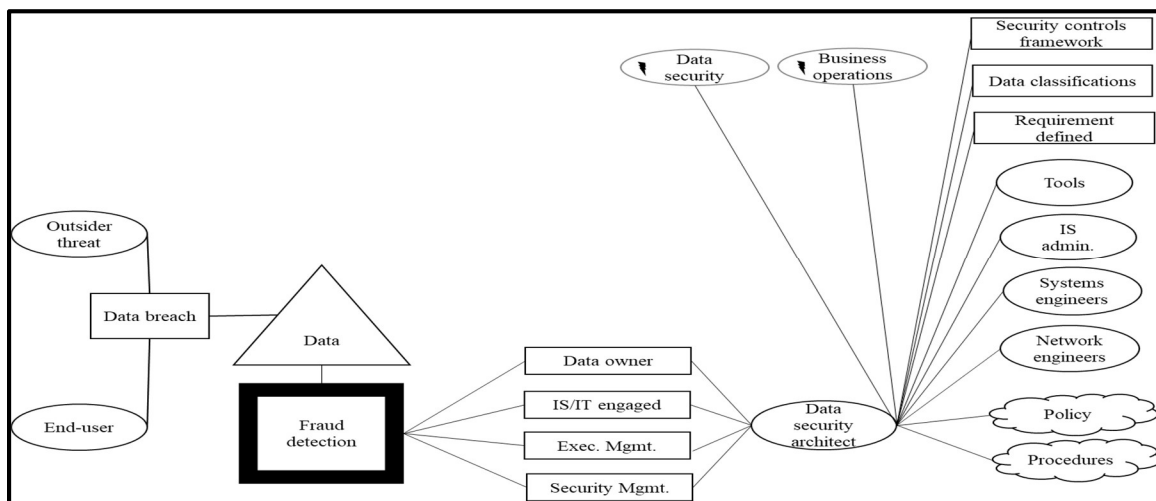


Figure 8. Encounter-episode 2 of architecture security strategy.

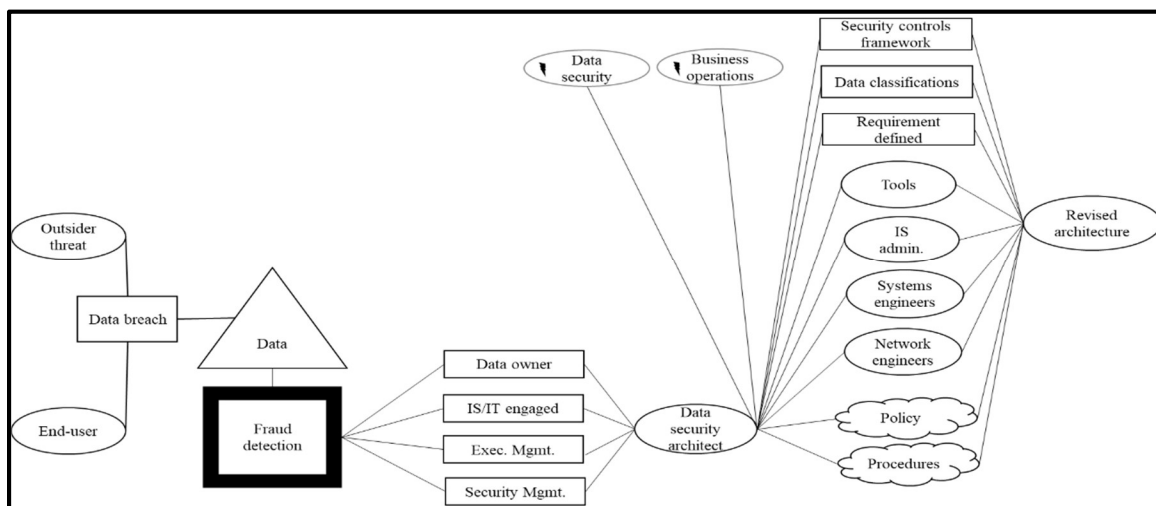


Figure 9. Encounter-episode 3 of architecture security strategy.

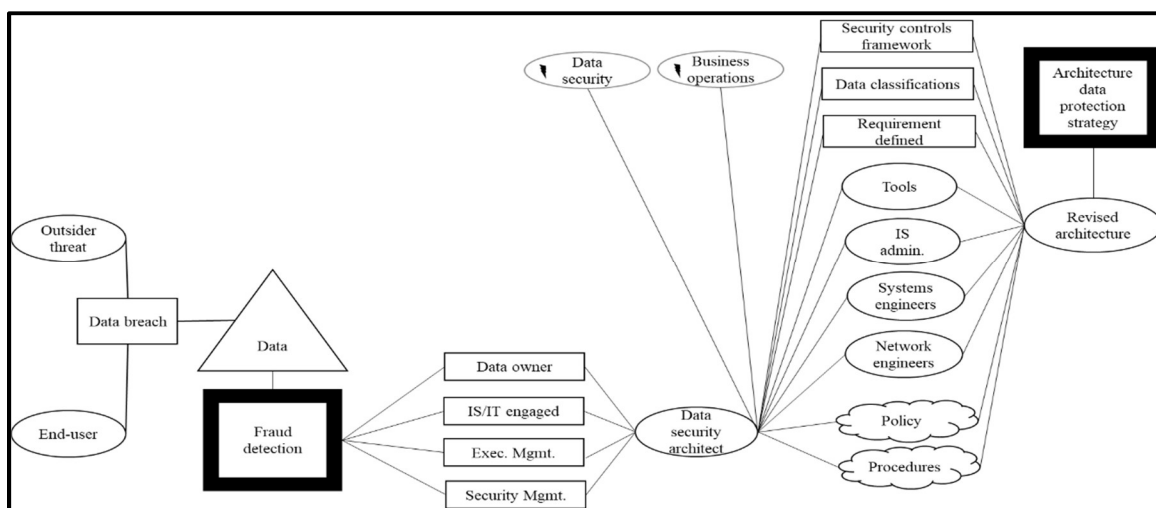


Figure 10. Encounter-episode 4 of architecture security strategy.

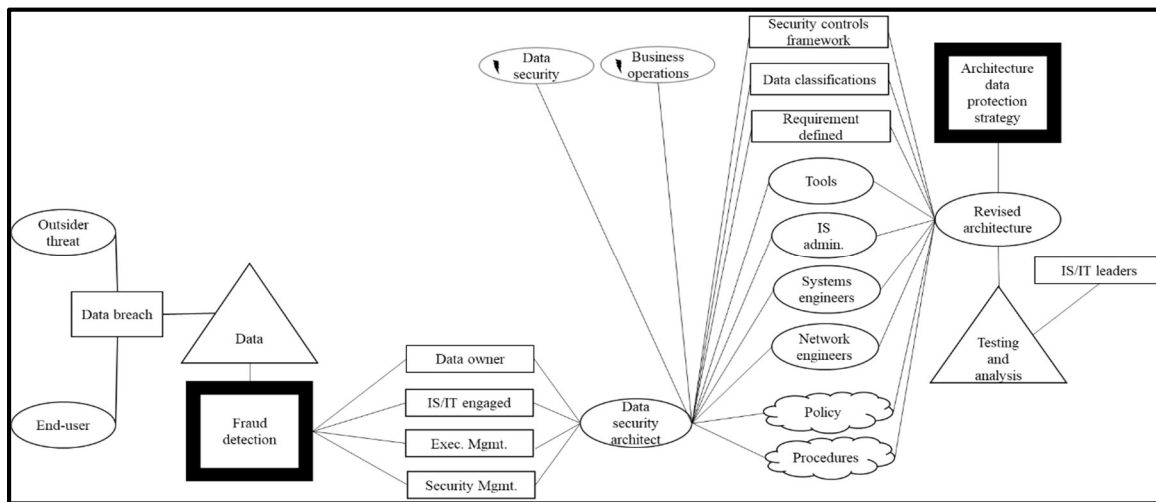


Figure 11. Encounter-episode 5 of architecture security strategy.

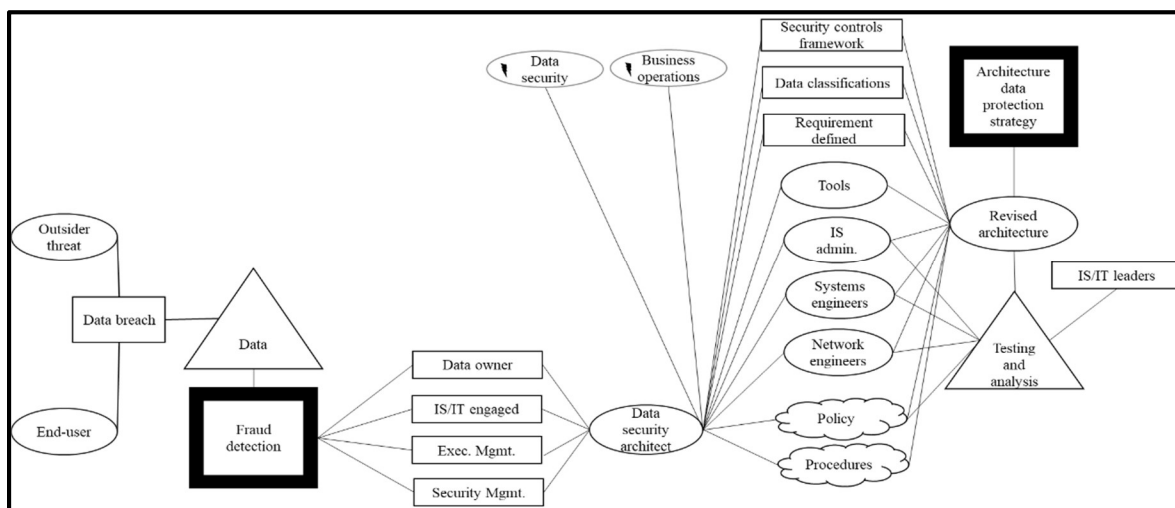


Figure 12. Encounter-episode 6 of architecture security strategy.

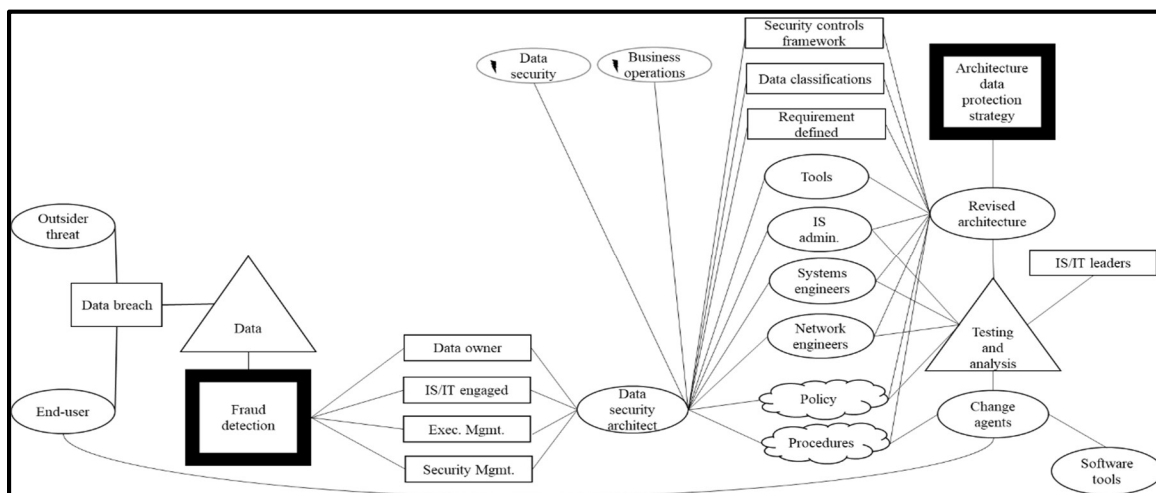


Figure 13. Encounter-episode 7 of architecture security strategy.

### Summary of the Findings

The purpose and significance of this study were supported by the overall research findings. Three overall themes emerged from the guiding data analyses of semistructured interviews, archival documents, and field notes. These three themes are *people* (i.e., security personnel, network engineers, system engineers, and qualified personnel to know how to monitor data); *processes* (i.e., the activities required to protect data from data loss); and *technology* (i.e., scientific knowledge used by people to protect data from data loss). The study findings from the ME partnering organization are indicative of successful application of data protection strategies that may be modeled using ANT-gs. The resulting ANT-gs models may be used as tools to assess vulnerabilities from technical and nontechnical threats to data impacting risk to business critical, sensitive, proprietary, and PII. The presentation of the findings was significant to answer the research question: “What strategies do ME business leaders use to improve data protection to reduce data loss resulting from cyberattacks?” ME business leaders



realizing the necessity for data protection may consider implementing the resulting strategies in their firms.

### **Applications to Professional Practice**

There are multiple applications to professional practice for ME business leaders in terms of protecting their data to reduce data loss resulting from cyberattacks. Applying the strategies from this study to professional practice is relative to the themes of *people* (i.e., security personnel, network engineers, system engineers, and qualified personnel to know how to monitor data); *processes* (i.e., inferring the activities required to protect data from data loss); and *technology* (i.e., inferring scientific knowledge used by people to protect data from data loss). It is important to understand that firm size does not impact the application of these data protection strategies to business practices (Saber, 2016). Yet, not implementing data protection strategies may lead to financial losses, legal ramifications, and a lack of or impact to competitive advantage (Alizadeh, Lu, Fahland, Zannone, & van der Aalst, 2018). These applications to professional practice are presented in terms of a procedural approach scenario and inserting the *why* and *how* with the strategies throughout the procedure.

Business leaders must evaluate the criticality of their data through data classification, ensuring alignment with their business strategies, and walking their business environment to see first-hand the lifecycle of the data. Saber (2016) found that data protection is critical to business survival and dependent on the integration of policy and training while Cook's (2017) findings underscored the importance of a strategic plan to provide a foundation for secure business operations. The evaluation to determine BCI

incorporates the threat and risk strategies. This *walk* is a physical action that means all stakeholders participate in the evaluation of the business data as it flows through the facility. Together, the stakeholders and business leaders work to determine the scope and scale of defining what is the BCI. This strategy is dependent on subject matter experts of the business data extending their knowledge to the people with the correct skill sets to assist in the determination of whether data is critical to the business and answering the *what if* questions associated with protecting the data (i.e., BCI) lifecycle. Participants related the walk to developing an understanding of the company infrastructure, business needs, system network and architecture, key challenges, available tools such as third-party vendor tools, existing security, and future security needs.

Business leaders and subject matter experts evaluate the most critical data in terms of threats. Threats in the coming 5G environment will increase with more opportunities for insider threats, scale (i.e., the types of threats), performance as more interconnectivity between devices (i.e., IoT), and applications (e.g., with increased bandwidth in 5G environments means new and emerging technologies; Suomalainen et al., 2018). The focus of this threat strategy is to ascertain the data essential to critical business activities related to the threat (Alizadeh et al., 2018). This strategy requires trained people knowledgeable in the types of technical and nontechnical threats specific to the business and the BCI. These skilled technicians relate the specific threats to the BCI to assess the existence of vulnerabilities and if there is risk that will impact the business and BCI. Participants related threat to the network, data movement, access to the data, people with need to know, technologies capable of detecting or identifying the

threat, training on what threats exist, different threat strategies, and again challenges with analyzing the threat.

Stakeholders, business leaders, and subject matter experts assess the security controls with the understanding of the threat. These risk, breach, and DLP strategies are combined and focused on mitigating vulnerabilities with an impact to the business. Risk mitigation requires a holistic approach including supplemental information such as times or locations of data and in doing so improves the accuracy of the security decisions (Sen & Borle, 2015). The breach strategy is about understanding the entry points to the network as it applies to the data. Businesses' reliance on their information systems to meet business requirements and obtain success is dependent on addressing the threats of breach (NIST, 2018). Incorporating a DLP strategy ensures security controls and protection measures are in place to restrict access to data and is crucial for protecting data. The use of a layered protection approach in terms of people with the correct skillsets, altering processes to minimize access and permissions to the data (i.e., aligning the policy, plans, standards and applications to support the processes), and incorporating a technological approach (i.e., software suites, technology tools, and IS/IT systems as a networked defense) through security awareness and training.

The final application to business of these study findings is for business leaders to continually monitor their data protection strategies for threat changes in terms of *people* (i.e., security personnel, network engineers, system engineers, and qualified personnel to know how to monitor data); *processes* (i.e., the activities required to protect data from data loss); and *technology* (i.e., scientific knowledge used by people to protect data from

data loss). This requires security awareness and education training to learn and develop people on the strategies selected for protecting the BCI. It requires ME leaders to invest in the selected processes through cost-benefit analyses in terms of continuing to protect against or recover against new or persistent threats. ME business leaders must apply these strategies to evolve with the technologies. Application of these various strategies may improve overall business performance as a direct result of improved financial health due to minimizing recovery costs from reduced data loss.

### **Implications for Social Change**

The foundational concept of ANT applies to the findings of this study and through a larger actor-network may impact social change. Impacting society for the purpose of social change is social shaping (Domínguez-Gómez, 2016). Domínguez-Gómez (2016) posited social shaping, in terms of ANT, as mobilizing actors and their relationships. Social change requires all elements of a network to be enrolled in the translations of the network for the envisioned desired outcomes (Shin & Lee, 2011). Social change inherently must modify networks (i.e., existing relationships), stakeholders (i.e., actors of those networks), and cause continuous chains of reactions (i.e., sociology of associations; Domínguez-Gómez, 2016; Shin & Lee, 2011). In terms of the findings from this study, ME business leaders adopting these data protection strategies mobilize their current networks and by action at a distance (i.e., continuous chains of reactions) influence other networks (Pestrol, 2006). Each data protection strategy to reduce data loss has meaning that is translated and perceived by individuals and collective groups of individuals. It is through these translations and perceptions of data protection strategies that the

implications of social change emerge. The chain reactions of these perceptions and implications materialize as positive social change in the form of altered attitudes toward data protection, creating a better environment for people to live and work; a reduction of recovery costs resulting from Internet crimes, improving social well-being; and enhancement of the methods used for the protection of sensitive, proprietary, and PII, that advances the privacy rights for society.

### **Recommendations for Action**

Recommendations (a) should flow logically from the conclusions and contain steps to useful action, (b) state who needs to pay attention to the results, and (c) indicate how the results might be disseminated via literature conferences and training. Several recommendations for action are suggested based on the findings from this study. These recommendations for action are made with the understanding that ME owners currently operate under a cybersecurity plan. ME owners may enhance current data security practices with following these recommendations for action.

I recommend the following actions based on the study findings:

- ME owners need to physically walk their data environments and learn what their BCI is and where it resides;
- ME owners need to inventory their people's skillsets, the processes currently used to support BCI, and the technology currently in place to support the people and processes;
- ME owners need to listen to the IS/IT leaders and decision makers concerning threats, vulnerabilities, and risks as it pertains to their BCI;

- ME owners need to evaluate threat as it pertains to 5G, IoT, and data portability as these are challenges facing the future of data protection;
- ME owners need to invest in specialized training for data protection professionals to develop and evolve these skillsets;
- ME owners need to align their system architectures to data protection strategies; and
- ME owners need to champion and support their IS/IT leaders and decision makers to create data protection as an organizational culture.

I intend to disseminate the findings of this study through industry publications and academic journals. I will also provide an informational sheet to the partnering organization. The information sheet will be communicated to the partnering organization as a tool they may share within their communities as ambassadors of data protection strategies. I intend to offer my services as a guest speaker to the following organizations: Florida Industrial Security Working Group, National Classification Management Society, and American Society for Industrial Security. Additionally, I plan to develop a video presentation of my research and findings for youtube.com.

### **Recommendations for Further Research**

As data breaches continue to occur and technology continues to evolve, the research into data protection strategies must keep pace to ensure individual privacy and business performance with financial health. Gwebu et al. (2018) reinforced this concern of data breaches growing frequency and the impact to afflicted firms with financial losses to include market share, sales, reputation, and consumer confidence. I recommend several

options for future research to develop the foundational work of this study. Several recommendations are a focus on improving the limitations of this study from Section 1. Other recommendations are addressing the delimitations of the study from Section 1. Finally, the remaining recommendations are for unique applications or working towards researching efficiencies in data protection.

This study was limited in several areas associated with the type of study, participants, and data collection instruments. A multiple case study with more than one organization may further the research on data protection strategies to reduce data loss from cyberattacks. A quantitative study is a means to quantify the findings of this research and may be appropriate for future research. Additionally, combining the qualitative and quantitative methodologies in a mixed-method approach may advance the research in data protection. This study limited the sample size to only five participants. A recommendation to increase the sample size may provide richer data and analysis. The population of this study was limited to only those in the IS/IT decision chain that were business leaders. Another recommendation is to expand the population to include the stakeholders, general business leaders in the firm, and the subject matter experts or data owners in future research. A final recommendation to address the limitation with the data collection instruments is to incorporate a survey prior to the semistructured interviews and archival document review. The survey is a key data collection for quantifying the collected data and improves the validity and reliability of the study.

This study was delimited in geography, business type, and industry. Delimiting the study to a small geographical area, a specific business type, and industry limits the

findings. The findings (i.e., a contextualized understanding) are of data protection strategies for a single ME with worldwide operations in Brevard County, Florida supporting the defense industry. Therefore, developing future research by expanding the geographical area first to a region versus a county broadens the understanding of data protection for a region. Scaling the research down to include small business or up to include large corporations broadens the context of knowledge to data protection strategies used in different business types. Finally, investigating other industries increases the understanding of data protection strategies to different industries to draw parallels or divergences.

There are unique applications for the findings in this study to support future research that may evolve data protection or find efficiencies. Data protection strategies in this study were modeled using the ANT-gs. The ANT-gs models might have application in risk-based scenarios. Risk-based regulation using data protection strategies is analogous to environmental regulation through environmental protection and citing non-compliance (Ceros, 2018; Gellert, 2015). The ANT-gs modeling of data protection strategies might prove foundational in developing algorithms for artificial intelligence applications. ANT-gs affords an understanding of the actors and actants in the network of data protection that future researchers might be able to harness to allow for artificial intelligence detection of new threat actors and through translation promulgate new actors and actants in a network response.



## Reflections

In my study, I acknowledged several assumptions to mitigate personal bias and I felt these held true for several reasons relative to the study findings. First, the semistructured interviews yielded enough themes, answered the overarching question, and supported triangulation. Second, face-to-face interviews with willing participants provided honest and direct responses. I felt these were honest as the responses confirmed large portions of my research. Third, I felt the findings provide value for business leaders to improve data protection and reduce data loss as the partnering organization has successfully implemented these strategies for over three years without data loss. Fourth, I furthered the research of Silvis and Alexander (2014) on the use of the conceptual framework of ANT through the ANT-gs and developed a usable ANT model and framework for data protection strategies that breaks down the complex nature of data protection to a visual procedural-based approach. Finally, the review of archival documents provided support to the triangulation of data and confirmed many aspects of the research to answer the research question.

Beginning the DBA process, I had preconceived ideas and concerns. I had notions that my preferences for quantitative research would negate my abilities to provide thoroughness in my qualitative approach to this study. My concerns were with the application of triangulation and my preconceived notion that quantitative research adds more rigor to answering a research question. This preconceived idea was due to my background as a scientist and quantitative researcher. I was surprised at the rigor I achieved in my applications of triangulating the data. Triangulation adds a level of

analyses I did not expect. I felt the selection of a qualitative study and incorporating triangulation with critical thinking truly broadened my results and experiences in research.

### **Conclusion**

The purpose of this qualitative, single case study was to explore the strategies ME business leaders use to improve data protection to reduce data loss from cyberattacks. I demonstrated with the findings of this study *why* and *how* some ME owners implement successful data protection strategies to reduce loss. These strategies are focused on countering threats to data, the mitigation of risks, understanding data breaches, incorporating DLP, and implementing notification and recovery processes. There are two desired outcomes from ME owners' implementation of these successful strategies. One, ME owners may catalyze business performance through improved business practices. Two, ME owners may influence social change through actions at a distance on sociotechnological networks.

The need to protect data is not a static event occurring in a specific space of time. Data protection is dynamic, evolving, and progresses regardless of time. Threats will continue to persist if technology continues to exist and evolve. Data protection strategies must keep pace with the ever-changing nature of technology. The strategies discussed in the study findings are about managing the risk to data to reduce data loss. Risk mitigation is controlling the consequences, minimizing the magnitude of the consequence, or preventing the occurrence of harm, damage, loss, or compromise to the data whether it is BCI, sensitive, proprietary, or PII. Understanding how the data may be breached assists

with implementing DLP. DLP is the means to safeguard and monitor data through the strategic use of people, processes, and technology. Notification and recovery are how the organization monitors and investigates breaches to the data. Business leaders must understand that data protection is knowing their data, the risks to their data, controlling the consequences associated with those risks through safeguarding, monitoring, and investigating the movement of the data.

## References

- Agelidis, Y. (2016). Protecting the good, the bad, and the ugly: Exposure data breaches and suggestions for coping with them. *Berkeley Technology Law Journal*, *31*, 1057-1078. doi:10.15779/Z38F28K
- Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., . . . Khan, M. K. (2015). Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation, and future directions. *Journal of Networks and Computer Applications*, *48*(February), 44-57. doi:10.1016/j.jnca.2014.10.009
- Alizadeh, M., Lu, X., Fahland, D., Zannone, N., & van der Aalst, W. M. P. (2018). Linking data and process perspectives for conformance analysis. *Computers & Security*, *73*(March 2018), 172-193. doi:10.1016/j.cose.2017.10.010
- Altman, M., Wood, A., O'Brien, D. R., & Gasser, U. (2018). Practical approaches to big data privacy over time. *International Data Privacy Law*, *8*, 29-51. doi:10.1093/idpl/ipx027
- Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*, 121-127. Retrieved from <http://tuckerpublish.com/jcd.htm>
- Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*, 893-916. Retrieved from <http://www.misq.org>
- Anugerah, D. P., & Indriani, M. (2018). Data protection in financial technology services

- (A study in Indonesian legal perspective). *Sriwijaya Law Review*, 2, 82-92.  
doi:10.28946/slrev.Vol2.Iss1.112.pp82-92
- Arbel, L. (2015). Data loss prevention: The business case. *Computer Fraud & Security*, 2015(5), 13-16. doi:10.1016/S1361-3723-(15)30037-3
- Aradau, C., & Blanke, T. (2015). The (big) data-security assemblage: Knowledge and critique. *Big Data & Society*, 2(2), 1-12. doi:10.1177/2053951715609066
- Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, 54, 46-56.  
doi:10.1080/01930826.2014.893116
- Ashenmacher, G. (2016). Indignity: Redefining the harm caused by data breaches. *Wake Forest Law Review*, 51, 1-56. Retrieved from <http://wakeforestlawreview.com>
- Au, M. H., Liang, K., Liu, J. K., Lu, R., & Ning, J. (2018). Privacy-preserving personal data operation on mobile cloud-chances and challenges over advanced persistent threat. *Future Generation Computer Systems*, 79, 337-349.  
doi:10.1016/j.future.2017.06.021
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253, 1-13.  
doi:10.1016/j.ejor.2015.12.023
- Barbour, J. B. (2017). Nutbags, enchiladas, and zombies: Marshaling narrative theory and practice for engaged research. *Management Communication Quarterly*, 31, 300-306. doi:10.1177/0893318916688091
- Baron, L. F., & Gomez, R. (2016). The associations between technologies and societies:

- The utility of actor-network theory. *Science, Technology, and Society*, 21, 129-148. doi:10.1177/0971721816640615
- Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods*, 27, 3-21. doi:10.1177/1525822X14526838
- Bartolini, C., & Siry, L. (2016). The right to be forgotten in the light of the consent of the data subject. *Computer Law & Security Review*, 32, 218-237. doi:10.1016/j.clsr.2016.01.005
- Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, 65(March 2017), 153-165. doi:10.1016/j.coso.2016.10.007
- Basias, N., & Pollalis, Y. (2018). Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. *Review of Integrative Business and Economics Research Methodology*, 7(s1), 91-105. Retrieved from <http://buscompress.com/journal-home.html>
- Baškarada, S. (2014). Qualitative case studies guidelines. *The Qualitative Report*, 19(40), 1-25. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Baskerville, R. L., & Myers, M. D. (2014). Design ethnography in information systems. *Information Systems Journal*, 25, 23-46. doi:10.1111/isj.12055
- Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information &*

*Management*, 51, 138-151. doi:10.1016/j.im/2013.11.004

Bellanova, R. (2016). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, 20, 329-347.

doi:10.1177/1368431016679167

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers on Human Behavior*, 48, 51-61.

doi:10.1016/j.chb.2015.01.039

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Journal of Nursing Plus Open*, 2(2016), 8-14.

doi:10.1016/j.npls.2016.01.001

Blome, C., Schoenherr, T., & Eckstein, D. (2014). The impact of knowledge transfer and complexity on supply chain flexibility: A knowledge-based view. *International Journal of Production Economics*, 147, 307-316. doi:10.1016/j.ijpe.2013.02.028

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

Bombak, A. E., & Hanson, H. M. (2016). Qualitative insights from the osteoporosis research: A narrative review of the literature. *Journal of Osteoporosis*, 2016, 1-

17. doi:10.1155/2016/7915041

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 58(7), 78-87.

doi:10.1145/2699390

Brody, B., Migueles, S. A., & Wendler, D. (2015). Should all research subjects be treated

- the same? *Hastings Center Report*, 45(1), 17-20. doi:10.1002/hast.414
- Burga, R., & Rezania, D. (2017). Project accountability: An exploratory case study using actor-network theory. *International Journal of Project Management*, 35, 1024-1036. doi:10.1016/j.ijproman.2017.05.001
- Callon, M., & Law, J. (1997). After the individual in society: Lessons from collectivity in science, technology and society. *Canadian Journal of Sociology*, 22, 165-182. doi:10.2307/3341747
- Calvard, T. S., & Jeske, D. (2018). Developing human resource data risk management in the age of big data. *International Journal of Information Management*, 43, 159-164. doi:10.1016/j.ijinfomgt.2018.07.011
- Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, 21(5), 811-831. Retrieved from <http://nsuworks.nova.edu/tqr/>
- 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
- Center for Development of Security Excellence. (2018). Insider threat indicators in user activity monitoring [Insider Threat Job Aid]. Retrieved from <https://www.cdse.edu/toolkits/insider/awareness.html>
- Ceross, A. (2018). Examining data protection enforcement actions through qualitative interviews and data exploration. *International Review of Law, Computers &*



*Technology*, 32, 99-117. doi:10.1080/13600869.2018.1418143

Chaudhary, R., Kumar, N., & Zeadally, S. (2017), Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges. *IEEE Communications Magazine*, 55(11), 114-122.  
doi:10.1109/MCOM.2017.1700102

Choi, S.-K., Yang, C.-H., & Kwak, J. (2018). System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats. *Transactions on Internet & Information Systems*, 12, 906-918. doi:10.3837/tiis.2018.02.022

Chu, H., & Ke, Q. (2017). Research methods: What's in the name? *Library and Information Science Research*, 39, 284-294. doi:10.1016/j.lisr.2017.11.001

Cibangu, S. K. (2013). A memo of qualitative research for information science: toward theory construction. *Journal of Documentation*, 69, 194-213.  
doi:10.1108/00220411311300048

Claus, B., Gandhi, R. A., Rawnsley, J., & Crowe, J. (2015). Using the oldest military force for the newest national defense. *Journal of Strategic Security*, 8(4), 1-22.  
doi:10.5038/1944-0472.8.4.1441

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588-608. Retrieved from <http://www.scirp.org>

Connelly, L. M. (2013). Limitation section. *Medsurg Nursing*, 22, 325-325, 336.  
Retrieved from <http://www.medsurnursing.net/cgi-bin/WebObjects/MSNJournal.woa>

- Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security*, 25, 118-136. doi:10.1108/ICS-03-2017-0013
- Cook, K. D. (2017). *Effective cyber security strategies for small businesses* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (UMI No. 10602149)
- Cresswell, K. M., Worth, A., & Sheikh, A. (2010). Actor-network theory and its role in understanding the implementation of information technology developments in healthcare. *BMC Medical Informatics and Decision Making*, 10(67), 1-11. doi:10.1186/1472-6947-10-67
- Crowley, M. G., & Johnstone, M. N. (2016). Protecting corporate intellectual property: Legal and technical approaches. *Business Horizons*, 59, 623-633. doi:10.1016/j.bushor.2016.08.004
- Dadelo, S., Turskis, Z., Zavadskas, E. K., & Dadeliene, R. (2014). Multi-criteria assessment and ranking system of sport team formation based on objective-measured values of criteria set. *Expert Systems with Applications*, 41, 6106-6113. doi:10.1016/j.eswa.2014.03.036
- 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
- Dasgupta, M. (2015). Exploring the relevance of case study research. *Vision*, 19, 147-

160. doi:10.1177/0972262915575661

Data Breach Accountability and Enforcement Act of 2017, S. 1900, 115th Cong. (2017, September 28). Retrieved from <https://www.congress.gov>

Desai, A., Zoccatelli, G., Adams, M., Allen, D., Brearley, S., Rafferty, A. M., ...

Donetto, S. (2017). Taking data seriously: The value of actor-network theory in rethinking patient experience data. *Journal of Health Services Research & Policy*, 22, 134-136. doi:10.1177/1355819616685349

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic insurance). *The Qualitative Report*, 21(3), 521-528. Retrieved from <http://nsuworks.nova.edu/tqr/>

Diorio, S. (2015). Data protection laws: Quilts versus blankets. *Syracuse Journal of International Law & Commerce*, 42, 485–513. Retrieved from <https://surface.syr.edu/jilc/>

Domínguez-Gómez, J. A. (2016). Four conceptual issues to consider in integrating social and environmental factors in risk and impact assessments. *Environmental Impact Assessment Review*, 56, 113-119. doi:10.1016/j.eiar.2015.09.009

Elder-Vass, D. (2015). Disassembling actor-network theory. *Philosophy of the Social Sciences*, 45, 100-121. doi:10.1177/0048393114525858

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337. Retrieved from <https://www.informingscience.org/Journals/IISIT/Overview>

- Engels, B. (2016). Data portability among online platforms. *Internet Policy Review*, 5(2), 1-17. doi:10.14763/2016.2.408
- Ernst & Young Global Limited. (2014). *Maximizing the value of data protection program* [Data file]. Retrieved from <http://ey.om/GRCinsights>
- Exec. Order No. 13556, 75 C.F.R. 68675-68677 (2010), retrieved from <https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information>
- Exec. Order No. 13800, 82 C.F.R. 22391-22397 (2017- 2018), retrieved from <https://www.federalregister.gov/presidential-documents/executive-orders/donald-trump/2017>
- Fan, K., Ren, Y., Wang, Y., Li, H., & Yang, Y. (2018). Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. *The Institute of Engineering and Technology*, 12, 527-532. doi:10.1049/iet-com.2017.0619
- Fang, D., Qian, Y., & Hu, R. Q. (2018). Security for 5G mobile wireless networks. *IEEE Access*, 6, 4850-4874. doi:10.1109/ACCESS.2017.2779146
- Federal Bureau of Investigation. (2017, March 8). FBI director addresses cyber security gathering: Varied group of cyber experts exchange ideas. Retrieved from the FBI.gov website: <https://www.fbi.gov/news/stories/fbi-director-addresses-cyber-security-gathering>
- FBI Internet Crime Complaint Center. (2015). *2015 Internet crime report* [Data file]. Retrieved from <https://www.ic3.gov/default.aspx>

FBI Internet Crime Complaint Center. (2016). *2016 Internet crime report* [Data file].

Retrieved from <https://www.ic3.gov/default.aspx>

FBI Internet Crime Complaint Center. (2017). *2017 Internet crime report* [Data file].

Retrieved from <https://www.ic3.gov/default.aspx>

Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3501 *et seq.*

(United States Publishing Office United States Code, 2017). Retrieved from <https://www.govinfo.gov>

Federal Trade Commission Act of 1938, 15 U.S.C.A. 41 *et seq.* (United States Publishing

Office United States Code, 2017). Retrieved from <https://www.govinfo.gov>

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision

support approaches for cyber security investment. *Decision Support Systems*, 86, 13-23. doi:10.1016/j.dss.2016.02.012

Fitzpatrick, W. M., & Dilullo, S. A. (2015). Cyber espionage and the S.P.I.E.S.

taxonomy. *Competition Forum*, 13(2), 307-336. Retrieved from <http://www.eberly.iup.edu/ASCWeb/>

Foresman, A. R. (2015). Once more unto the [corporate data] breach, dear friends.

*Journal of Corporation Law*, 41, 343-358. Retrieved from <http://jcl.law.uiowa.edu>

Freitas, F., Ribeiro, J., Brandão, C., Reis, L. P., de Souza, F. N., & Costa, A. P. (2017).

Learn by yourself: The self-learning tools for qualitative analysis software packages. *Digital Education Review*, 32(December 2017), 97-117. Retrieved from <http://revistes.ub.edu/index.php/der/index>

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative

- research. *The Qualitative Report*, 20(9), 1408-1416. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Gayomali, C. (2014). Why do companies keep getting hacked? Retrieved from <http://www.fastcompany.com/3026672/the-code-war/why-do-companies-keep-getting-hacked>
- Gellert, R. (2015). Data protection: A risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law*, 5, 3-19. doi:10.1093/idpl/ipu035
- Gentles, S. J., Charles, C., Ploeg, J., & McKibbin, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, 20(11), 1772-1789. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Ghafoor, A., Sher, M., Imran, M., & Derhab, A. (2015). Secure key distribution using fragmentation and assimilation in wireless sensor and actor networks. *International Journal of Distributed Sensor Networks*, 11, 1-13. doi:10.1155/2015/542856
- Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research*, 11, 517-525. doi:10.1080/19361610.2016.1211876
- Government Accountability Office. (2015a). *Federal information security actions needed to address challenges* (GAO Highlights GAO-15-725T). Retrieved from Government Accountability Office website: <http://www.gao.gov/>
- Government Accountability Office. (2015b). *Information security: Cyber threats and*

*data breaches illustrate need for stronger controls across federal agencies* (GAO Highlights GAO-15-758T). Retrieved from Government Accountability Office website: <http://www.gao.gov/>

- Graneheim, U. H., Lindgren, B. M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today, 56*, 29-34. doi:10.1016/j.nedt.2017.06.002
- Green, C. A., Duan, N., Gibbons, R. D., Hoagwood, K. E., Palinkas, L. A., & Wisdom, J. P. (2015). Approaches to mixed methods dissemination and implementation research: Methods, strengths, caveats, and opportunities. *Administration and Policy in Mental Health and Mental Health Services Research, 42*, 508-523. doi:10.1007/s10488-014-0552-6
- Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems, 35*, 683-714. doi:10.1080/07421222
- Hanseth, O., Aanestad, M., & Berg, M. (2004). Guest editors' introduction: Actor-network theory and information systems. What's so special? *Information Technology & People, 17*, 116-123. doi:10.1108/09593840410542466
- Hare, S. (2016). For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection. *Business Horizons, 59*, 549-561. doi:10.1016/j.bushor.2016.04.002
- Hausken, K. (2014). Returns to information security investment: Endogenizing the expected loss. *Information Systems Frontiers, 16*, 329-336. doi:10.1007/s10796-

012-9390-9

- Heeney, C. (2017). An “ethical moment” in data sharing. *Science, Technology, & Human Values, 42*, 3-28. doi:10.1177/0162243916648220
- Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*(February 2016), 30-38. doi:10.1016/j.techsoc.2015.11.007
- Hintze, M. (2018). Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the GDPR. *Journal of Internet Law, 22*(2), 17-31. doi:10.2139/ssrn.3192721
- Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management, 52*, 337-347. doi:10.1016/j.im.2014.12.006
- Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior, 37*, 353-367. doi:10.1080/01639625.2015.1026766
- Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*, 585-591. doi:10.1016/j.bushor.2016.07.004
- Hossain, M. A., & Dwivedi, Y. K. (2014). What improves citizens’ privacy perceptions toward RFID technology? A cross-country investigation using mixed methods approach. *International Journal of Information Management, 34*, 711-719. doi:10.1016/j.ijinfomgt.2014.07.002



- Hubaux, J.-P., & Juels, A. (2016). Viewpoint: Privacy is dead, long live privacy, protecting social norms as confidentiality wanes. *Communications of the ACM*, 59(6), 39-41. doi:10.1145/2834114
- Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for identifying cybersecurity risks in manufacturing. *Procedia Manufacturing*, 1, 47-63. doi:10.1016/j.promfg.2015.09.060
- Hardy, L. J., Hughes, A., Hulen, E., & Schwartz, A. L. (2016). Implementing qualitative data management plans to ensure ethical standards in multi-partner centers, *Journal of Empirical Research on Human Research Ethics*, 11, 191-198. doi:10.1177/1556264616636233
- Hung, A. C. Y. (2017). Beyond the player: A user-centered approach to analyzing digital games and players using actor-network theory. *E-Learning and Digital Media*, 13, 227-243. doi:10.1177/2042753017691655
- ITL Bulletin. (2012, June). *Cloud computing: A review of features, benefits, and risks, and recommendations for secure, efficient implementations*. Retrieved from Information Technology Laboratory website: <https://www.nist.gov/itl>
- 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
- Jackson, B. (2018). The changing research data landscape and the experiences of the ethics review board chairs: Implications for library practice and partnerships. *The*

*Journal of Academic Librarianship*, 44, 603-612.

doi:10.1016/j.acalib.2018.07.001

Jackson, S. (2015). Toward an analytical and methodological understanding of actor-network theory. *Journal of Arts & Humanities*, 4(2), 29-44.

doi:10.18533/journal.v4i2.210

Jacobs, B., & Popma, J. (2019). Medical research, big data and the need for privacy by design. *Big Data & Society*, 6(1), 1-5. <https://doi.org/10.1177/2053951718824352>

Jadhav, V., Kumar, K. N., Alias Rana, P. D., Seetharaman, A., Kalia, S., & Maddulety, K. (2017). Understanding the correlation among factors of cyber systems security for Internet of things (IoT) in smart cities. *Journal of Accounting, Business & Management*, 24(2), 1-15. Retrieved from <http://journal.stie-mce.ac.id/index.php/jabminternational/index>

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, 20, 196-213.

doi:10.1080/02681102.2013.814040

Johnson, M., O'Hara, R., Hirst, E., Weyman, A., Turner, J., Mason, S., . . . Siriwardena, A. N. (2017). Multiple triangulation and collaborative research using qualitative methods to explore decision making in pre-hospital emergency care. *Journal of BMC Medical Research Methodology*, 17(2017), 11-22. doi:10.1186/s12874-017-0290-z

- Kauffman, L., Lesser, N., & Abe, B. (2015). *Executive technical workshop on improving cybersecurity and consumer privacy* (NIST IR 8050). Retrieved from National Cybersecurity Center of Excellence website:  
[https://nccoe.nist.gov/sites/default/files/nccoe/NISTIR\\_8050\\_draft\\_1.pdf](https://nccoe.nist.gov/sites/default/files/nccoe/NISTIR_8050_draft_1.pdf)
- Kaukola, J., Ruohonen, J., Tuomisto, A., Hyrynsalmi, S., & Leppänen, V. (2017). Tightroping between APT and BCI in small enterprises. *Information & Computer Security*, 25, 226-239. doi:10.1108/ICS-07-2016-0047
- Kelly, J. D., Branham, L., & Decker, M. R. (2016). Abducted children and youth in Lord's Resistance Army in Northeastern Democratic Republic of the Congo (DRC): Mechanisms of indoctrination and control. *Conflict and Health*, 10(2016), 1-11. doi:10.1186/s13031-016-0078-5
- Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU member states. *Computer Law & Security Review*, 32, 91-110. doi:10.1016/j.clsr.2015.12.004
- Kongnso, F. (2015). *Determining small business cybersecurity strategies to prevent data breaches* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global (UMI No. 3739769)
- Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, 28, 159-171. doi:10.1080/13600869.2013.801589
- Kruth, J. G. (2015). Five qualitative research approaches and their applications in

- parapsychology. *Journal of Parapsychology*, 79, 219-233. Retrieved from <http://www.parapsych.org>
- Kuang, L., Zhu, Y., Li, S., Yan, X., Yan, H., & Deng, S. (2018). A privacy protection model of data publication based on game theory [Article ID 3486529]. *Security and Communication Networks*, 2018, 1-13. doi:10.1155/2018/3486529
- Kuhn, T. (1970). *The structure of scientific revolutions* (2nd ed.) [Adobe Acrobat Reader]. Chicago, IL: University of Chicago Press. Retrieved from [https://projektintegracija.pravo.hr/\\_download/repository/Kuhn\\_Structure\\_of\\_Scientific\\_Revolutions.pdf](https://projektintegracija.pravo.hr/_download/repository/Kuhn_Structure_of_Scientific_Revolutions.pdf)
- 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. (1996). On actor-network theory. A few clarifications plus more than a few complications [Data file]. *Soziale Welt*, 47, 369-381. Retrieved from <http://www.soziale-welt.nomos.de/>
- Latour, B. (2011). Networks, societies, spheres: Reflections of an actor-network theorist. *International Journal of Communication*, 5, 796-810. Retrieved from <http://ijoc.org/index.php/ijoc/index>
- Lavastre, O., Gunasekaran, A., & Spalanzani, A. (2012). Supply chain risk management in French companies. *Decision Support Systems*, 52, 828-838. doi:10.1016/j.dss.2011.11.017
- Law, J. (2008). On sociology and STS. *Sociological Review*, 56, 623-649.

doi:10.1111/j.1467-954X.2008.00808.x

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, 19, 321-330.

doi:10.1016/j.jisa.2014.10.012

Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. *Information Management & Computer Security*, 21, 420-443. doi:10.1108/IMCS-04-2013-0027

Lie, R., & Witteveen, L. (2017). Visual informed consent: Informed consent without forms. *International Journal of Social Research Methodology*, 20, 63-75.

doi:10.1080/13645579.2015.1116835

Lupton, D. (2016). Digital companion species and eating data: Implications for theorizing digital dat0human assemblages. *Big Data & Society*, 3(1), 1-5.

doi:10.1177/2053951715619947

Ma, F. (2015). A review of research methods in EFL education. *Theory and Practice in Language Studies*, 5, 566-571. doi:10.17507/tpls.503.16

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education*, 9, 33501-33514. Retrieved from <https://www.ojs.aishe.org>

Mähring, M., Holmström, J., Keil, M., & Montealegre, R. (2004). Trojan actor-networks and swift translation: Bringing actor-network theory to IT project escalation

studies. *Information Technology & People*, 17, 210-238.

doi:10.1108/09593840410542510

Malecki, F. (2014). The cost of network-based attacks. *Network Security*, 2014(3), 17-18.

doi:10.1016/S1353-4858(14)70033-9

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. J. (2013). Does sample size matter in qualitative research?: A review of qualitative interviews in is research. *Journal of Computer Information Systems*, 54(1), 11-22.

doi:10.1080/08874417.2013.11645667

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.

doi:10.1509/jm.15.0497

McDermid, F., Peters, K., Jackson, D., & Daly, J. (2014). Conducting qualitative research in the context of pre-existing and collegial relationships. *Nurse Researcher*, 21(5), 28-33. Retrieved from <http://www.nursing-standard.co.uk>

Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review*, 4(10), 33-39. Retrieved from <http://timereview.ca>

Mitchell, A. (2016). GDPR: Evolutionary or revolutionary? [Opinion piece]. *Journal of Direct, Data and Digital Marketing Practice*, 17, 217-221. doi:10.1057/s41263-016-0006-9

Morse, J. M. (2015). Data were saturated. *Qualitative Health Research*, 25, 587-588.

doi:10.1177/1049732315576699

- Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research*, 19, 129-132. doi:10.1177/1362168815572747
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1*. Gaithersburg, MD. doi:10.6028/NIST.CSWP.04162018
- National Intellectual Property Rights Coordination Center. (2015). *2015 special 301 report* [Data file]. Retrieved from <https://www.iprcenter.gov/reports/ipr-center-reports/2015-special-301-report/view>
- Naude, M. J., & Chiweshe, N. (2017). A proposed operational risk management framework for small and medium enterprises. *South African Journal of Economic and Management Sciences*, 20, 1-10. doi:10.4102/sajems.v20i1.1621
- Neal, P., & Ilsever, J. (2016). Protecting information: Active cyber defense for the business entity: A prerequisite corporate policy. *Academy of Strategic Management Journal*, 15(2), 15-35. Retrieved from <http://www.alliedacademies.org/academy-of-strategic-management-journal/>
- Neusar, A. (2014). To trust or not to trust? Interpretations in qualitative research. *Human Affairs*, 24, 178-188. doi:10.2478/s13374-014-0218-9
- Newton, V. L. (2017). 'It's good to be able to talk': An exploration of the complexities of participant and researcher relationships when conducting sensitive research. *Woman's Studies International Forum*, 61(2017), 93-99. doi:10.1016/j.wsif.2016.11.011
- Ngulube, P. (2015). Trends in research methodological procedures used in knowledge

- management studies. *African Journal of Library, Archives and Information Science*, 25, 125-143. Retrieved from <https://www.ajol.info/index.php/ajlais>
- O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by design: Informed consent and Internet of things for smart health. *Procedia Computer Science*, 113, 653-658. doi:10.1016/j.procs.2017.08.329
- Office of Human Research Protections. (2016). *The Belmont Report: Ethical principals and guidelines for the protection of human subjects of research*. Retrieved from <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>
- Office of the Federal Register. (2017). *Office policy for the protection of human subjects* [Data file]. Retrieved from <https://www.federalregister.gov/documents/2017/01/19/2017-01058/federal-policy-for-the-protection-of-human-subjects>
- Office of the Law Revision Counsel. (2018a). United States code. Retrieved from U.S. House of Representatives website <https://www.uscode.house.gov>
- Office of the Law Revision Counsel. (2018b). United States Constitution [Data file]. Retrieved from <http://uscode.house.gov/static/constitution.pdf>
- Olaniyi, O. M., Folorunso, T. A., Aliyu, A., & Olugbenga, J. (2016). Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach. *International Journal of Information Engineering and Electronic Business*, 8(5), 9-17. doi:10.5815/ijieeb.2016.05.02
- Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretation of verbal and nonverbal data in qualitative research.



*International Journal of Education*, 6(1), 183-246. doi:10.5296/ije.v6i1.4399

Onwuegbuzie, A. J., & Hwang, E. (2014). Interviewing successfully for academic positions: A framework for candidates for asking questions during the interview process. *International Journal of Education*, 6(2), 98-113.

doi:10.5296/ije.v6i2.4424

Orlu, A. D. (2016). Information seeking behavior of masters students: Affective and behavioural dimensions [Paper 1387]. *Library Philosophy and Practice (e-journal)*. Retrieved from <http://digitalcommons.unl.edu/libphilprac/1387>

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems*, 92(2016), 47-56. doi:10.1016/j.dss.2016.09.012

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. *Administrative and Policy in Mental Health and Mental Health Services Research*, 42, 533-544. doi:10.1007/s10488-013-0528-y

Parent, M., & Cusack, B. (2016). Cybersecurity in 2016: People, technology, and processes. *Business Horizons*, 59, 567-569. doi:10.1016/j.bushor.2016.08.005

Park, S.-Y., Shon, C., Kwon, O. Y., Yoon, T. Y., & Kwon, I. (2017). A qualitative thematic content analysis of medical students' essays on professionalism. *BMC Medical Education*, 17(1), 79-84. doi:10.1186/s12909-017-0920-5

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information

security questionnaire (HAIS-Q). *Computers & Security*, 42(May 2014), 165-176.

doi:10.1016/j.cose.2013.12.003

Pawlowski, S. D., & Jung, Y. (2015, Fall). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education*, 26, 281-294. Retrieved from <http://jise.org/Volume26/index.html>

Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report*, 20(2), 76-85. Retrieved from <http://nsuworks.nova.edu/tqr/>

Peredaryenko, M. S., & Krauss, S. E. (2013). Calibrating the human instrument: Understanding the interviewing experience of novice qualitative researchers. *The Qualitative Report*, 18(43), 1-17. Retrieved from <http://nsuworks.nova.edu/tqr/>

Perkmann, M., & Schildt, H. (2015). Open data partnerships between firms and universities: The role of boundary organizations. *Research Policy*, 44, 1133-1143. doi:10.1016/j.respol.2014.12.006

Pickering, L., & Kara, H. (2017). Presenting and representing others: Towards an ethics of engagement. *International Journal of Social Research Methodology*, 20, 299-309. doi:10.1080/13645579.2017.1287875

Pipelines: Securing the veins of the American economy: Hearings before the Subcommittee on Transportation Security of the Committee on Homeland Security, House of Representatives, 114th Cong. 1-14 (2016, April 19). (testimony of Paul W. Parfomak).

- Plachkinova, M., & Maurer, C. (2018). Teaching case security breach at Target. *Journal of Information Systems Education*, 29, 11-19. Retrieved from <http://www.jise.appstate.edu>
- Ponemon Institute. (2014). Fourth annual benchmark study on patient privacy & data security [Data file]. Retrieved from <https://www.ponemon.org/>
- Ponemon Institute. (2016). 2016 cost of cyber crime study & risk of business innovation [Data file]. Retrieved from <https://www.ponemon.org/>
- Popescul, D., & Radu, L. D. (2016). Data security in smart cities: Challenges and solutions. *Informatica Economica*, 20(1), 29-38.  
doi:10.12948/issn14531305/20.1.2016.03
- Posner, B. Z. (2016). Investigating the reliability and validity of the leadership practices inventory. *Administrative Sciences*, 6(4), 1-23. doi:10.3390/admsci6040017
- Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal of Accounting Information Systems*, 20(2016), 38-64.  
doi:10.1016/j.accinf.2016.01.004
- Rose, N., & Miller, P. (1992). Political power beyond the state: Problematics of government. *The British Journal of Sociology*, 43, 173-205. doi:2307/591464
- Rimando, M., Brace, A., Namageyo-Funa, A., Parr, T. L., Sealy, D.-A., Davis, T. L., ... Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *The Qualitative Report*, 20(12), 2025-2036. Retrieved from <http://nsuworks.nova.edu/tqr/>

- Ryan, G. W., & Bernard, H. R. (2003). Techniques to identify themes. *Field Methods, 15*, 85-109. doi:10.1177/155822X02239569
- Rumbold, J. M. M., & Pierscionek, B. K. (2018). What are data? A categorization of the data sensitivity spectrum. *Big Data Research, 12*(2018), 49-59. doi:10.1016/j.bdr.2017.11.001
- Saber, J. (2016). *Determining small business cybersecurity strategies to prevent data breaches* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global (UMI No. 10181342)
- Safarzadeh, A., Shafipour, V., & Salar, A. (2018). Expectant mothers' experiences with lay doulas in maternity units of hospitals in impoverished areas of Iran: A qualitative study. *Iranian Journal of Nursing & Midwifery Research, 23*, 437-443. doi:10.4103/ijnmr.IJNMR\_109\_17
- Salim, H. (2014). *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks* (Working Paper CISL # 2014-07). Retrieved from <http://web.mit.edu/smadnick/www/wp/2014-07.pdf>
- Salmona, M., & Kaczynski, D. (2016). Don't blame the software: Using qualitative data analysis software successfully in doctoral research. *Forum: Qualitative Social Research, 17*(3), 42-64. doi:10.17169/fqs-17.3.2505
- Salviulo, F., & Scanniello, G. (2014). Dealing with identifiers and comments in source code comprehension and maintenance: Results from an ethnographically-informed study with students and professionals. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*,

48. doi:10.1145/2601248.2601251

- Sapat, A., Schwartz, L., Esnard, A., & Sewordor, E. (2017). Integrating qualitative data analysis software into doctoral public administration education. *Journal of Public Affairs Education, 23*, 959-978. doi:10.1080/15236803.2017.12002299
- Sarabdeen, J., & Moonesar, I. A. (2018). Privacy protection laws and public perception of data privacy: The case of Dubai e-health care services. *Benchmarking: An International Journal, 25*, 1883-1902. doi:10.1108/BIJ-06-2017-0133
- Sarma, S. K. (2015). Qualitative research: Examining the misconceptions. *South Asian Journal of Management, 22*(3), 176-191. Retrieved from <http://www.sajm-andisa.org>
- Sayes, E. (2014). Actor-network theory and methodology: Just what does it mean to say that nonhumans have agency? *Social Studies of Science, 44*, 134-149. doi:10.1177/030631271351186
- Sayin, H. U. (2016). A short introduction to system theory: Indispensable postulate systems and basic structures of the systems in quantum physics, biology and neuroscience. *NeuroQuantology, 14*, 126-142. doi:10.14704/nq.2016.14.1.855
- Schubert, D. F., Cedarbaum, J. G., & Schloss, L. (2015). The SEC's two primary theories in cybersecurity enforcement actions. *The Cybersecurity Law Report, 1*(1), 1-6. Retrieved from <http://www.cslawreport.com>
- Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*, 314-341. doi:10.1080/07421222.2015.1063315

- Shin, D.-H., & Lee, C.-W. (2011). Disruptive innovation for social change: How technology innovation can be best managed in social context. *Telematics and Informatics*, 28, 86-100. doi:10/1016/j.tele.2010.08.002
- Shordike, A., Hocking, C., Bunrayong, W., Vittayakorn, S., Rattakorn, P., Pierce, D., & Wright-St Clair, V. A. (2017). Research as relationship: Engaging with ethical intent. *International Journal of Social Research Methodology*, 20, 299-309. doi:10.1080/13645579.2017.1287875
- Silvis, E., & Alexander, P. M. (2014). A study using a graphical syntax for actor-network theory. *Information Technology & People*, 27, 110-128. doi:10.1108/ITP-06-2013-0101
- Simon, M. K., & Goes, J. (2003). *Assumptions, limitations, delimitations, and scope of the study* [Data file]. Retrieved from <http://www.dissertationrecipes.com>
- Singh, S., Corner, P. D., & Pavlovich, K. (2015). Failed, not finished: A narrative approach to understanding venture failure stigmatization. *Journal of Business Venturing*, 30, 150-166. doi:10.1016/j.jbusvent.2014.07.005
- Small Business Administration. (2017). *Table of small business size standards* [Data file]. Retrieved from <https://www.sba.gov/contracting/getting-started-contractor/make-sure-you-meet-sba-size-standards/table-small-business-size-standards>
- Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, 75(July 2015), 49-62. doi:10.1016/j.dss.2015.04.011

- Sullivan, R. J., & Maniff, J. L. (2016). Data breach notification laws. *Economic Review* (01612387), *101*(1), 65-85. Retrieved from <https://www.kansascityfed.org/>
- Suomalainen, J., Ahola, K., Majanen, M., Mämmelä, O., & Ruuska, P. (2018). Security awareness in software-defined multi-domain 5G networks [Article 27]. *Future Internet*, *10*(3), 1-24. doi:10.3390/fi10030027
- Tanev, G., Tzolov, P., & Apiafi, R. (2015). A value blueprint approach to cybersecurity in networked medical devices. *Technology Innovation Management Review*, *5*(6), 17-25. Retrieved from <http://timereview.ca>
- Thumlert, K., de Castell, S., & Jenson, J. (2015). Short cuts and extended techniques: Rethinking relations between technology and educational theory. *Educational Philosophy and Theory*, *47*, 786-803. doi:10.1080/00131857.2014.901163
- Trafimow, D. (2014). Considering quantitative and qualitative issues together. *Qualitative Research in Psychology*, *11*, 15-24. doi:10.1080/14780887.2012.743202
- Tran, V.-T., Porchar, R., Tran, V.-C., & Ravaud, P. (2017). Predicting data saturation in qualitative surveys with mathematical models from ecological research. *Journal of Clinical Epidemiology*, *82*(2017), 71-78. doi:10.1016/j.jclinepi.2016.10.001
- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*, 38-58. doi:10.1057/ejis.2013.27
- Tu, M., Spoa-Harty, K., & Xiao, L. (2015). Data loss prevention and control: inside activity incident monitoring, identification, and tracking in healthcare enterprise

environments. *Journal of Digital Forensics, Security and Law*, 10(1), 27-44.

Retrieved from <http://www.jdfsl.org/index.htm>

Ursic, H. (2018). Unfolding the new-born right to data portability: Four gateways to data subject control. *Script-ed: A Journal of Law, Technology & Society*, 15(1), 42-69. doi:10.2966/scrip.150118.42

Vanberg, A. D. (2018). The right to data portability in the GDPR: What lessons can be learned from the EU experience?. *Journal of Internet Law*, 21(7), 1-19. Retrieved from <http://ejlt.org/article/view/546/726>

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology*, 18(2018), 148. doi:10.1186/s12874-018-0594-7

Väyrynen, K., Hekkala, R., & Liias, T. (2013). Knowledge protection challenges of social media encountered by organizations. *Journal of Organizational Computing and Electronic Commerce*, 23, 34-55, doi:10.1080/10919392.2013.748607

Vicsek, L., Király, G., & Kónya, H. (2016). Networks in social sciences: Comparing actor-network theory and social network analysis. *Corvinus Journal of Sociology and Social Policy*, 7(2), 77-102. doi:10.14267/CJSSP.2016.02.04

Vitel, P., & Bliddal, H. (2015). French cyber security and defense: An overview. *Information & Security: An International Journal*, 32, 29-41. doi:10.11610/isij.3209

Von Bertalanffy, L. (1968). *General systems theory: Foundations, development,*



*application* (Rev. ed.). New York, NY: George Braziller.

- Walls, D. M. (2015). Access(ing) the coordination of writing networks. *Computers and Composition, 38*, 68-78. doi:10.1016/j.compcom.2015.09.004
- Wang, X., Chen, F., Ye, H., Yang, J., Zhu, J., Zhang, Z., & Huang, Y. (2017). Data transmission and access protection of community medical Internet of things. *Journal of Sensors, 2017*, 1-14. doi:10.1155/2017/7862842
- Whitler, K. A., & Farris, P. W. (2017). The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research, 57*, 3-9. doi:10.2501/JAR-2017-005
- Willan, M. M. (2016). Research approaches for higher education students: A personal experience. *BCES Conference Proceedings, 14*, 247-254. Retrieved from <http://bces-conference.org/>
- Wu, J.-S., Lin, C.-T., Lee, Y.-J., & Chong, S.-K. (2015). Keystroke and mouse movement profiling for data loss prevention. *Journal of Information Science and Engineering, 31*, 23-42. Retrieved from <http://jise.iis.sinica.edu.tw/>
- Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.-K., & Gao, X. (2018). A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications, 36*, 679-695. doi:10.1109/JSAC.2018.2825560
- Xu, M. A., & Storr, G. B. (2012). Learning the concept of researcher as instrument in qualitative research. *The Qualitative Report, 17*(21), 1-18. Retrieved from <http://nsuworks.nova.edu/tqr/>

- Yan, Z., Li, X., & Kantola, R. (2015). Controlling cloud data access based on reputation. *Mobile Networks & Applications*, 20, 828-839. doi:10.1007/s11036-015-0591-6
- Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, 20(2), 134-152. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, 48, 311-325. doi:10.1111/ejed.12014
- Yin, R. K. (2014). *Case study research: Design and methods (5th ed.)*. Thousand Oaks, CA: Sage.
- Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015). A theory of cyber attacks: A step towards analyzing MTD systems. *MTD '15 Proceedings of the second ACM Workshop on Moving Target Defense, USA*, 11-20. doi:10.1145/2808475.808478
- Zuva, T., Esan, O. A., & Ngwira, S. M. (2014). Hybridization of bimodal biometrics for access control authentication. *Internal Journal of Future Computer and Communication*, 3(6), 444-451. doi:10.7763/IJFCC.2014.V3.344

## Appendix A: Interview Protocol

Study Title: Strategies for Improving Data Protection to Reduce Data Loss from  
Cyberattacks

Date: \_\_\_\_\_

Researcher: \_\_\_\_\_

### Pre-Interview Checklist

1. Introduce self to participant and ask informal ice breaker to put participant at ease.
2. Express appreciation to participant.
3. Verify receipt and/or response to the Participant Informed Consent Form, and ask if they retained the original copy, or need a replacement copy of the signed form, then answer any questions and/or concerns of participant.
4. Get confirmation and acknowledgement that interview is being recorded.
5. Turn on recording device.
6. Start interview with restating the research objective.
7. Follow interview protocol through to closing comments.

### Interview Questions

1. What strategies have you used to improve data protection to reduce data loss resulting from cyberattacks?
2. What strategies did you find worked best to improve data protection to reduce data loss resulting from cyberattacks?

3. What are some examples of technical threats to your firm's data that influenced your selection of strategies to improve data protection to reduce data loss resulting from cyberattacks?
4. What are some examples of nontechnical threats to your firm's data that influenced your selection of strategies to improve data protection to reduce data loss resulting from cyberattacks?
5. What, if any, types of training were offered or required for your personnel to contribute to the implementation of the selected strategies?
6. How did you determine your chosen strategies were successful at improving data protection and reducing data loss?
7. How did you address key challenges to implementing your chosen strategies to improve data protection to reduce data loss?
8. Do you have any additional information you wish to contribute that you have not previously addressed about improving data protection to reduce data loss resulting from cyberattacks?

#### Closing Interview Checklist

End interview and terminate recording.

Thank the participant again for participating in the study. Confirm the participant contact information for follow up questions and concerns.

Provide researcher contact information with Walden University (i.e., email and phone contact).

Discuss member checking with participant to include time required for it, the forthcoming letter, and participant responsibilities in response to the letter.

Solicit any final questions or concerns, close out the interview.

End protocol.

## Appendix B: Member Checking Letter

Date:

Subject: Member Checking of Interview Transcript Analysis

Dear Participant:

As we discussed towards the end of your interview, attached is the data analysis file from the recorded interview session. Please review and provide your concurrence of the analysis within 1 business day. Please provide email response of acceptance to the following researcher email ( ).

If questions or concerns exist with the analysis, please provide your additional input via email at the email address provided above.

Feel free to contact me with any questions or concerns using the researcher email ( ).

Respectfully,

Encl (1)

## Appendix C: Observation Protocol

Study Title: Strategies for Improving Data Protection to Reduce Data Loss from  
Cyberattacks

Date: \_\_\_\_\_ Researcher: Jennifer E. Cannon

Tools for Observation Protocol:

Plain pad of paper and pencil.

Protocol for observations:

1. Observe initial aspects of the environment (i.e., lighting, temperature, and furniture).
2. Observe initial appearance of interview (i.e., professional attire, business attire, etc.).
3. Observe baseline reactions to introductory conversation during rapport building stage of interview (i.e., relaxed or nervous).
4. Observe interviewee verbal cues (i.e., amount of detail, speech errors, speech fillers, pauses, and voice tone).
5. Observe interview non-verbal cues (i.e., eye contact, facial expression, gestures, body language, voice, and verbal style).
6. Observe researcher reactions throughout the interview (i.e., jot key words, record feelings associated with an interviewee's response, record physical state of researcher, general impression about the quality of the interview responses).

End protocol.

## Appendix D: Journaling Protocol

Study Title: Strategies for Improving Data Protection to Reduce Data Loss from  
Cyberattacks

Date: \_\_\_\_\_ Researcher: Jennifer E. Cannon

Tools for Journaling Protocol:

1. Evernote Application.
2. Plain pad of paper and pencil in the event Microsoft Surface experiences power or other technical issues preventing use of the notetaking app.

Protocol for Journaling with Evernote:

1. Create a *notebook* for observations and journaling of interviews associated with study.
2. Title the notebook with the study title as noted above in this protocol.
3. Use individual notes to identify the different interviewees (i.e., interviewee P1, interviewee P2, etc.).
4. Create tags for searching the material later.
5. Transcribe Evernote notes immediately upon completion of interview.
6. Do not edit notes taken during the interview.
7. Write in first and third person.
8. Use real time and end point descriptions.

Protocol for Journaling with pad/pencil:

1. Create journal index. Place *Index* at the top of the first two pages.



2. Number remaining pages in the notebook (i.e., 1, 2, 3, etc.) to serve as the journal pages immediately following the second index page.
3. Create the schedule of interviews page to document the date, time, and place for the agreed upon interviews. Place *Schedule of Interviews* on page 3.
4. Create the notetaking space for each interviewee. Place *Interviewee P1* on page 4. Place quadrants on the page to allow for notetaking associated with the observation protocol (i.e., six quadrants to correspond with the six observation protocols). Allow enough pages to capture additional notes that exceed the page 4 six quadrants. Place *Interviewee P1 continued* on additional pages used for notetaking. Follow the same process for each interviewee.
5. Transcribe journal notes immediately upon completion of interview.
6. Do not edit notes taken during the interview.
7. Write in first and third person.
8. Use real time and end point descriptions.

End protocol.