2019

Strategies to Reduce the Fiscal Impact of Cyberattacks

Shirley Denise Smith
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Shirley D. Smith

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. Denise Land, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Jamiel Vadell, Committee Member, Doctor of Business Administration Faculty

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

The Office of the Provost

Walden University
2019

Abstract

Strategies to Reduce the Fiscal Impact of Cyberattacks

by

Shirley D. Smith

MBA, Walden University, 2011

BS, Jackson State University, 1980

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration-Entrepreneurship

Walden University

October 2019

Abstract

A single cyberattack event involving 1 major corporation can cause severe business and social devastation. In this single case study, a major U.S. airline company was selected for exploration of the strategies information technology administrators and airline managers implemented to reduce the financial devastation that may be caused by a cyberattack. Seven participants, of whom 4 were airline managers and 3 were IT administrators, whose primary responsibility included implementation of strategies to plan for and respond to cyberattacks participated in the data collection process. This study was grounded on the general systems theory. Data collection entailed semistructured face-to-face and telephone interviews and collection and review of public documents. The data analysis process of this study involved the use of Yin’s 5-step process of compiling, disassembling, reassembling, interpreting, and concluding, which provided a detailed analysis of the emerging themes. The findings produced results that identified strategies organizational managers and administrators of a U.S. airline implemented to reduce the fiscal influence of cyberattacks, such as proactive plans for education and training, active management, and an incident response plan. The findings of this study might affect social change by offering all individuals a perspective on creating effective cyberculture. An understanding of cyberculture could include the focus of a heightened understanding, whereby, to ensure the security of sensitive or privileged data and information and of key assets, thus, reducing the fiscal devastation that may be caused by cyberattacks.

Strategies to Reduce the Fiscal Impact of Cyberattacks

by

Shirley D. Smith

MBA, Walden University, 2011

BS, Jackson State University, 1980

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2019

Dedication

This research is dedicated to my loving parents, the late Clarence and Lenora Monix. It was embedded in my mentality from a small child that I would go to college, but I never thought that I would find myself on the journey to obtain a doctorate. My father was a businessperson and an entrepreneur. Unbeknownst to me, he was grooming me for business for years by having me read contracts and follow him on his business dealings. To my angels, thank you for watching over me, and to you, I genuinely give all that I have become.

Acknowledgments

I want to take this opportunity to render acknowledgments to Dr. Denise Land, my esteemed chair. It was Dr. Land, who accepted me into her classroom late in my doctoral program. She challenged me to elevate my work by engaging in a more profound and synthesized research and introducing me to valuable resources to achieve that goal. Above all else, Dr. Land exemplified patience with me at times that I was upset with myself. I would also like to acknowledge my siblings as we warmly refer to ourselves, "The Terrific Ten." Special thanks to my sister, Dr. Demetria Monix-Goode, who discussed with me all of the reasons why I should pursue my DBA and provided undying support as I went through the program. Thanks to my husband and my sons, who understood those times I was unable to participate in some family events. Lastly, I acknowledge Dr. Carol Miller, my mentor, and friend. I wish Dr. Miller nothing but blessings upon her retirement with over 30 years in higher education.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Cyberattacks, as they relate to aviation have given rise to a new paradigm in the realm of cybersecurity, and pose a threat on the ground and in the air (Pollard & Clark, 2019). The digital revolution has created a society with an ever-increasing need for technology. A study by Huang, Siegel, and Madnick (2018) indicated that 61% of CEOs are concerned about the impact of cyberattacks on their organizations. By conducting a qualitative, single case study involving one major airline, I explored strategies to reduce the fiscal impact cyberattacks can have on all industries.

Background of the Problem

Cyberattacks have the potential to destroy important and confidential information, communication systems, infrastructure, and psychological operations. Munkhdorj and Yuji (2017) discussed the term zero-day vulnerability as this describes the period between when the vulnerability was discovered and the first attack. The number of intended cyberattacks against organizations increases daily (Munkhdorj & Yuji, 2017). Zero-day vulnerabilities, which take advantage of security susceptibilities, more than doubled with a 125% increase from 2014 to 2015; thus, the average rate of occurrence for a new zero-day vulnerability was found to be weekly in 2015 (Munkhdorj & Yuji, 2017). The serious consequences that a cyberattack could have on critical infrastructure make it an extreme threat with the potential to cripple transportation (Ntalampiras, 2015). Outcomes such as this demonstrate the primary reason computer professionals have a significant role in the discussion of cyberattacks as they are relied on daily to help with these problems (Hsu, Tsaih, & Yen, 2018). The growing dependence on technology and issues associated with it have made cyberattacks a significant concern in the airline industry.

A primary U.S. airline incurred a system failure that disabled operations of the carrier for hours and caused canceled flights. Fox (2016) suggested that organizations should place the focus not only on eliminating errors but should also direct attention towards being resilient when dealing with unknown and unstable factors. The same carrier had also been compromised in April, 2015, when someone publicly tweeted information regarding the ability to infiltrate in-flight security and control an aircraft (Holt, Moallemi, Weiland, Earnhardt, & McMullen, 2016). An inquiry was made to a group of boards of directors to determine what it is that causes the most challenges, which Greene, Gupta, L'Helias, and McCracken (2017) identified as security issues. Greene et al. explained the board members have a lack of understanding in that area and an unwillingness to take the time to gain an understanding. It is because of the potential devastation, lack of knowledge, and financial implications of a cyberattack that continued research is vital.

Problem Statement

Organization leaders have either encountered a cyberattack or are waiting to incur a cyberattack (Huang et al., 2018). Also, Huang et al. (2018) advised that the cost of the cyber-phenomenon has been estimated to have increased from $3 trillion in 2015 to $6 trillion by 2021. In 2016, losses related to the breach of corporate data totaled $95,869,990 (Federal Bureau of Investigation, Internet Crime Complaint Center, 2017). The general business problem is that the inability to improve cyber resiliency can lead to economic loss for some airlines. The specific business problem is that some information technology (IT) administrators and airline managers lack effective strategies to reduce the fiscal impact of cyberattacks.

Purpose Statement

The purpose of this qualitative single case study was to explore the strategies IT administrators and airline managers use to reduce the fiscal impact of cyberattacks. In this study, the population included IT administrators and management from one major U.S. airline who have used strategies to reduce the fiscal impact of cyberattacks. This study may contribute to positive social change by enhancing the knowledge of IT administrators, airline managers, and researchers. The implementation of enhanced knowledge could prompt legislators to understand the need for new cyber laws. With the passing of new and updated regulations, consumers, primarily in the airline industry, could benefit from the presence of a safe and secure environment. New regulations could bring the consumers comfort in knowing there is the protection of their personal information and transportation.

Nature of the Study

Qualitative research is a method that researchers use to capitalize on observations from data and to deliver abstracted knowledge; moreover, qualitative research offers challenging insights to existing theories and divulges new ones (Bansal, Smith, & Vaara, 2018). When implementing the qualitative method, researchers usually associate it with the questions of what and why (Barnham, 2015). Quantitative researchers, conversely, analyze numerical data using statistical methods (Starr, 2014). Uprichard and Dawney

(2019) shared that mixed-method researchers combine the quantitative and qualitative methods for addressing the same research question. The mixed-method approach is presumed valuable because it can capture the complexity of the social world more accurately than a single research method might (Uprichard & Dawney, 2019); however, only one approach was needed in this research as the experiences of airline managers and IT administrators can be best explored with the qualitative method. For this study, employing the qualitative approach allowed me to conduct interviews and gather data through which I was able to obtain a clear picture of the participants' experiences, determinants that cannot be met by examining the statistical significance of relationships or differences among variables as required by quantitative and mixed method approaches.

Commonly used qualitative design strategies include phenomenology, ethnography, and case study (Moser & Korstjens, 2018). Lichterman (2017) shared that researchers use ethnography when they wish to immerse themselves within the domain of a group of people who share the same culture or lived experience; this type of research was designed to study people in their environment. This study did not require me to be immersed among the participants; therefore, ethnography was not a practical choice for this research. When researchers use the phenomenological design, the researcher can explore the meaning of the participants' lived experiences, which allows the use of criterion sampling whereby the participants meet a predefined criterion (Moser & Korstjens, 2018). Further, use of the phenomenological design allows the researcher to identify the lived experience related to the specified phenomenon to frame the thoughts and perceptions from the perspective of the participant (Mayoh & Onwuegbuzie, 2015).

The focus of this study was not on what the participants experienced of the phenomena, and therefore the phenomenological design was also not applicable to this study. I used a single case study design. I eliminated the phenomenological and ethnography models because I chose to disengage my assumptions and biases and embraced the case study design. The case study design is an exploration of skills, knowledge, and strategies (Moser & Korstjens, 2018). I selected this design because it aligned with the purpose of my study. The data collection strategy I used allowed me to collect in-depth content and ensured findings that provided rich data. I used a qualitative case study to explore strategies that IT administrators and airline managers use to reduce the fiscal impact of cyberattacks.

Research Question

The research question guiding this study was:

What strategies do IT administrators and airline managers use to reduce the fiscal impact of cyberattacks?

Interview Questions

1. What strategies are currently in place to reduce the fiscal impact of cyberattacks?
2. How have cyberattacks affected or altered your department’s processes?
3. How do you assess the effectiveness of the strategies you have implemented to reduce cyberattacks?
4. What were the key barriers to implementing the strategies you have established to reduce the impact of cyberattacks?

5. How did you address the obstacles to implementing these strategies?
6. How did the agents respond to the procedures that were implemented in past cyber-situations?
7. What information can you add to this interview that I may not have addressed?

Conceptual Framework

The conceptual foundation for this study was von Bertalanffy’s (1972) general systems theory, which is a concept where individuals should view security as a whole system through both design and operation. Burns (2016) introduced the chaos theory in which decisions may influence external forces and cause an organization to become disrupted. Burns believed management is responsible for managing the execution of all of the moving parts. The systems approach encompasses the process in establishing the system and the ongoing management process for ensuring the system’s reliability (Burns, 2016), expanding on von Bertalanffy’s theory. General systems theory and the chaos theory apply to this study because their combined general concepts support the idea that for a security system to be effective, strategies to prevent and address security threats through a systems approach is needed.

Operational Definitions

Cyber activities: Cyber activities refer to the encroachment of various types of tactics and procedures on a system. The assailant may have the goal of inflicting disruption or, in some cases, propaganda, whereby, there is an attempt to influence public opinion or disrupt the victims’ finances. Also included in this category of activities are the compromising of private information and stalking online publication content (Kostyuk & Zhukov, 2019).

Cyberattack: A cyberattack is an intentional mishandling of computer systems and networks. This attack may include altering or stealing information on program data and financial information from organizations or individuals. Additionally, cyberattacks may disrupt or sabotage the victims' ability to operate in the physical or electronic realm and may be launched by anyone at any time (Sibi Chakkaravarthy, Sangeetha, Venkata Rathnam, Srinithi, & Vaidehi, 2018).

Cybercrimes: Cybercrimes are the manipulation of technology for a selfish purpose, which could involve surveillance, medical research, political repression, blackmail, or ill-gained profits (Trotter & Chythlook, 2016). These illegal activities are conducted through electronic mechanisms such as computers, mobile devices, and other network tools. A wide variety of criminal activity is covered under this label including sending or spreading viruses, hacking, spamming, phishing, and obtaining unauthorized access to other systems to steal financial information (Ali, 2019).

Cyberespionage: Cyberespionage is spying technology that permits information to be gathered by searching through a competitor's system in an illegal intelligence gathering activity (Bressler & Bressler, 2015). In simpler terms, it may be considered as the theft of intellectual property and company secrets in cyberspace. The monitoring of systems and information gathering are the main motivation; thus, the espionage attackers' goal is to steal valuable information, obtain technical advantages, or to gain the upper hand in a future negotiation. It is common for the attacker to be looking for specific information (Wangen, 2015).

Cyber hacker: A cyber hacker is an individual who accesses a computer system by circumventing the security system of the affected organization (Bressler & Bressler, 2015). The hacker may also be identified as a malicious hacker who uses digital tools to conduct destructive attacks against organizations who rely on technology. Hackers purposely take advantage of computer system weaknesses and may use malicious tools such as Ransomware, Zeus, Trojans, and Keyloggers (Samtani, Chinn, Chen, & Nunamaker, 2017).

Cyber resiliency: Cyber resiliency may be used as a secondary approach to cybersecurity whereby the focus is placed on training staff to recognize attempts of social engineering, phishing attempts, and how to report an incident in the event of a suspicious activity or stolen equipment (Brown, 2016). Resiliency is the ability to recover or fight through a cyberattack or random event and requires more than having secure systems. Resiliency also requires a plan for recovery from an event through the creation of affordable, trustworthy, and resilient strategies (Mailloux & Grimaila, 2018).

Cybersecurity: Cybersecurity is the central proponent in operation and maintenance of the security of an organization. It involves the study of threats associated with cyber and provides defensive solutions to cyberattacks. Security solutions are of utmost importance because of the impact it could make globally, such as protecting Internet-connected systems in the event of cyberattacks (Dan-Suteu, 2018).

Data breach: Data breach is the exposure of essential or sensitive data by identity theft. In 2014, 17.6 million individuals were victimized in the United States (Sullivan & Maniff, 2016). One of the most devastating types of cyber events includes data breaches. Between 2005 and 2017, 7,730 violations occurred, which accounts for 9,919,228,821 breached records; furthermore, the average global cost in 2016 was also significant in regard to stolen records of sensitive or confidential information (Maochao, Schweitzer, Bateman, & Shouhuai, 2018).

Human factor: The human factor may be referred to as a malicious insider. The human factor may be an employee or an individual who has access to the confidential information of an organization and violates the security policies (Liang, Biros, & Luse, 2016). The human factor is a severe threat to the organization, more so than the outsider because of the insider's easy access to private information. Even though many organizations have sophisticated security mechanisms to detect the outsider, very few tools have been established for preventing attacks by the human factor of the insider (Smrithy, Cuzzocrea, & Balakrishnan, 2018).

Phishing: Phishing involves the use of social engineering techniques to imitate electronic communications from a trustworthy source and steal credentials, collect private information, or install malicious software (Jensen, Dinger, Wright, & Thatcher, 2017). Phishing may take the form of unsolicited e-mails resembling legitimate messages. If the unsuspecting individual falls for the attack, the phisher may then sell the information, commit identity theft, or commit financial fraud or other cybercrime (Jensen et al., 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions in a study may be articulated or unarticulated. Nkwake and Morrow (2016) identified assumptions as beliefs, expectations, or considerations that are taken for granted. Assumptions may be valid, or they may not be accurate; however, they are things outside of the researcher's control believed to be true (Marshall & Rossman, 2016). There were three assumptions for this study. My first assumption was interviewing IT administrators and airline managers would be the best research design to gain information related to the research question. I also needed to assume the participants were answering honestly and without reservation. Lastly, I assumed the emerging themes and patterns gathered from data analysis would provide the information necessary to address the research question.

Limitations

Limitations may be viewed as things outside of the researcher's control that may limit the scope of the research findings. Limitations for this study included lack of available documents, participants who lived the phenomenon, and the data collection process; additionally, there may be the inclusion of biases from the researcher and a break in the accuracy (Yin, 2018). I understood the probability of encountering similar limitations in this study. A potential weakness of the proposed research was the small sample size. Another limitation was the qualitative single case study design, which had the potential to limit the insights gathered from the study findings. By conducting interviews to collect data, information may have been excluded that could have been obtained from other research methods.

Delimitations

This study was delimited to exploring strategies IT administrators and airline managers at a single U.S. airline use to reduce the fiscal impact of cyberattacks. Delimitations establish the limit of the scope or boundaries of the study (Marshall & Rossman, 2016). Delimitations were in my control as the researcher because I could make choices to determine them. Liao and Hitchcock (2018) stated delimitations make it possible for the researcher to decide what problem they wish to investigate, what research questions to ask, the theoretical perspectives to embrace, and the participants to select. In terms of the boundaries, delimitations also relate to the geographic location I selected, which was the United States. Scope is the inclusiveness of data and extends not only to the boundary but to the details of the topic; in other words, all aspects of the phenomenon are explored (Morse, 2015).

Significance of the Study

Contribution to Business Practice

By identifying effective strategies to reduce the impact of cyberattacks, airline managers and IT administrators could prevent millions of dollars of lost revenue. Cyberattacks against government entities and private companies such as the airline industry continue to increase in number (Melnik, 2015). Considering the increasing amount of lost revenue by organizations because of cyberattacks, this study may add value because it identifies strategies that may be implemented to reduce the fiscal impact.

Large organizations with revenues over $1 billion reported that financial losses due to cyber incidents increased from $3.9 million in 2013 to $5.9 million in 2014 (Melnik, 2015). The price of a lack of resiliency in response to an event can be devastating; this study highlights the need for education and training to promote preparation and resiliency. This study could also cause a shift in the mindset of management to place a higher priority on cyber security as part of normal business practices.

Implications for Social Change

The findings from this study could contribute to social change by bringing a heightened awareness of the need for a cyberculture. Cyberculture is an environment in which attention is placed on cyber health, reducing the costs resulting from cyber incidents and perhaps mitigating the need for individuals to purchase cyber insurance. In the cyberculture environment, individuals would become educated regarding cyberattacks. Education on the phenomena would help individuals to recognize phishing and other fraudulent efforts and to use antivirus software. It has been estimated that four to five new malware variants were discovered every second in 2016 (Major, 2017). By embracing a cyberculture, individuals could develop a strong desire to create a business environment that promotes preparedness and resiliency.

Lastly, the implementation of a cyberculture could prompt legislators to understand the need for new cyber laws. With the passing of new and updated regulations, consumers could benefit from the presence of a safe and secure environment. New regulations could bring the consumers comfort in knowing there is the protection of their personal information and transportation.

A Review of the Professional and Academic Literature

A well-constructed literature review is important to researchers because it provides an updated and clear overview of the literature applicable to a specific area of study, adding value to the work. The purpose of performing a review is that it allows the researcher to refresh familiarity with the reference material and to return to reference material in an organized manner (Wee & Banister, 2016). The research question that guided this study asked: What strategies can the IT administrators in the airline industry implement to reduce the fiscal impact of cyberattacks.

In compiling this study, the databases used included Google Scholar, EBSCOhost, and ProQuest. Key search words include *cyber activities, cyberattacks, cybercrimes, cyberespionage, cyber hacker, cyber resiliency, cybersecurity, data breach, human factor,* and *phishing.* These terms were selected because of the way they relate to the subject matter. The terms cover various aspects of understanding cyber incidents and strategic planning for prevention and response. I used Google Scholar linked with the Walden University online library as my primary search engine to find scholarly articles to add context to the foundation of this study. The completed study included 188 references of which 171 of the references count as peer-reviewed, representing 93% of the total. I used Ulrich's serials analysis system website to ensure the articles were peer-reviewed. I minimized the percentage of references more than 5 years from the anticipated date of chief academic officer (CAO) approval. The total references published within the past 5 years totaled 163, which is 87% of the total number of references. The literature review section consists of 83 total references, of which 76 (91%) are peer-reviewed , and 85.5 %

were published within 5 years of anticipated CAO approval date. The references also include several non-peer-reviewed and peer-reviewed articles such as government sources and seminal works to show the history of a conceptual framework or to add historical context.

The purpose of this qualitative, single case study was to explore the strategies that IT administrators and airline managers use to reduce the fiscal impact of cyberattacks. This literature review was guided by this purpose and began with an in-depth look at the conceptual framework, which was grounded on the von Bertalanffy's (1972) general systems theory. In this theory, systems should be viewed as a whole unit to address an event. Cybersecurity centers have begun to combine preventive and reactive security measures to establish a more inclusive and expanded view of security. These centers have been considered as some of the most successful in cybersecurity management because in alignment with the general systems theory; their views originate from a holistic perspective (Backman, 2015). In addition to the literature regarding the conceptual framework is literature related to security and prevention, an overview of cyberattacks, the effect of management, IT personnel, internal threats, financial implications, and the role of cyber laws.

Conceptual Framework Theory Considerations

There have been many theories that address the growing issue of the various systematic aspects of cyber security. Theories addressed in this section include general systems theory, which is the basis of the conceptual framework, with emphasis on the security decay theory. I discuss correlating theories, including complexity theory, chaos theory, social media theory, production theory, and multilayer security theory. Also shared are contrasting theories highlighting disruptive innovation and security and prevention. The conceptual framework theory for this study was based on the general systems theory (von Bertalanffy, 1972), wherein systems and operations must be viewed holistically, as an entire unit. Hammad and Hallinger (2017) advised that the conceptual framework is often used in qualitative research to deliver in-depth understanding and insight into the key issue being studied.

Von Bertalanffy (1972), an Austrian biologist, was responsible for developing the general systems theory based upon the thought that individuals should view a single element in the context of its relationship to the system within which it resides (Morgeson, Mitchell, & Liu, 2015). Morgeson et al. (2015) also advised that systems theory is applicable to organizational (social) phenomena, whereas traditional systems tend to focus on the environment, teams, organizations, and individuals and not considering events. One of the advantages of implementing the general systems theory is it may aid organizational leaders in adapting to environmental changes, making decisions in terms of the macro as well as the microenvironment. A disadvantage may be that adopting such a view may not necessarily be a practical way to lead because it may delay the decision-making process. Burns (2016) introduced the chaos theory in which small external forces are believed to be a major force in altering a system and even influencing critical decisions. The external forces could also cause an air of chaos; thus, leaders of organizations must be mindful of delivering the proper measures for the specific situation. Burns provided a positive aspect to his theory when he mentioned the forces could also generate sustainability and lead the individual to a broader foundation from which to make critical decisions.

In order to deliver a robust conceptual framework, the researcher should extract concepts from more than a single theory, which is a strategy that I used. Antonino (2015) indicated that by using a variety of ideas, the research is strengthened and provides a more profound understanding; also, scholars agree that the conceptual framework is a critical aspect of disciplined inquiry, and it serves as a link between relevant concepts, theories, and empirical evidence to form the research question or selection of methods (Antonino, 2015). I framed my research question and researched theories to support my potential findings. It is pertinent for researchers to consider the works of other scholars to create a clear picture of the topic (Dasgupta, 2015). Additionally, the researcher should provide patterns that produce themes and illustrate a detailed representation of the phenomenon (Onwuegbuzie & Weinbaum, 2017). In the conceptual framework for this study, I included theories that correlated with and contrasted to the general systems theory. Information contained within this conceptual framework was designed to provide scholars with insight into and new consideration of cybersecurity and strategies that may be implemented to reduce the fiscal impact of a cyberattack.

General systems theory. In this study, the conceptual framework was based on von Bertalanffy’s (1972) theory that suggests individuals should view security as a whole-system problem in design and operation. One approach embraced by von Bertalanffy was to have the researcher focus on the universe and select general phenomena from many different disciplines, then build general theoretical models relevant to the phenomena, such as evolution, and define a general system as any theoretical system of interest to more than one discipline. This new vision of reality is based on awareness of the essential interrelatedness and interdependence of all phenomena; thus, systems are integrated wholes whose properties cannot be reduced to those of smaller units. Von Bertalanffy discovered the need for the consciousness of a general system is a matter of life and death, not just for individuals but also for future generations.

As a researcher, von Bertalanffy (1972) had mixed thoughts regarding the general systems theory in relation to cybernetics. Cybernetics is important to this framework because it is a new field of science that unites the human context of thinking and engineering, as this science was created to combine the functions of automatic machines and the nervous system (Drack & Pouvreau, 2015). Von Bertalanffy did think cybernetics fell short of being a general systems theory but appreciated cybernetics in regard to its insight into regulatory behavior and addressing the phenomena of unknown systems. Von Bertalanffy's interest exceeded the technical or formal aspects of theory and extended into philosophy and worldview.

The general systems theory was not isolated as a new discipline. The work of von Bertalanffy (1972) was in alignment with the research of Ashby (1991), who was also concerned with cybernetics and how each part of a system affects the other. Ashby ascertained that understanding feedback from a system is not enough and cannot be treated as separate parts but only as a whole unit. Ashby also theorized there must be an understanding of general principles of dynamic systems; otherwise, feedback alone is unimportant. Furthermore, the importance lies within the complex systems that offer cross-connectivity internally. There has been some criticism of the general systems theory and its proponents in that it may not apply to smaller organizations and only to large, complex systems (Morgeson et al., 2015).

Security decay theory. Coole and Brooks (2014) developed a theoretical foundation of security decay from the perspectives of defense-in-depth (DID) and von Bertalanffy's (1972) general systems theory. DID is pertinent to this study as it encourages a holistic approach to security decay and the systems approach; ultimately, both processes must be present in establishing the system and the ongoing management processes that aim to ensure the system reliability delivers over time (Coole & Brooks, 2014). The researchers found DID is a strategy that can be hindered by actions of decay and disorganization, supporting entropy, in which case the DID elements must be maintained at optimum operating levels. Yong-Jun and Deng-Feng (2016) defined entropy as the amount of information produced by a random process; thus, the more expansive the value, the more uncertainty exists. Entropy measures the energy of thermodynamic variables such as temperature, pressure, and composition. Coole and Brooks concluded this could lead to a reduction in overall system performance, which could be avoided at the stage design through compelling risk identification. They also advocated active monitoring and reviewing of treatment strategies.

Introduction of correlating theories. Several correlating theories were also considered for the conceptual framework for this study. The correlated theories relate to and expand upon the concepts presented by von Bertalanffy's (1972) systems theory and security decay theory (Coole & Brooks, 2014). The theories considered included social media theory (Mangal, 2013), complexity theory (Cairney, 2012), and multilayer security theory (Lee & Kang, 2015).

Social media theory. There are over 2 billion Internet users who log more than 142,460,000,000 hours per month online, making the Internet a crucial part of life. Social media is so prevalent on the Internet that an estimated 49.3% of the top 10,000 websites in the world have links to Facebook, the most popular social networking website (Mangal, 2013). Social media theory by Mangal (2013) embraces the general systems theory of von Bertalanffy (1972) and correlates with the theory of Coole and Brooks (2014), who strongly supported the case that elements of a system must be maintained at optimum operating levels. Mangal indicated websites possessing debilitated components were inferior and made for negative user experience, and the information security elements should include collaboration between IT administrators and integration the proper preventions tools to minimize threats. Mangal defined a system as a group of elements that are organized in an order that corresponds with the overall function of the system. The elements interact with each other and with entities within the system with the purpose of being resilient, organized, and able to grow or diversify. Resilience, hierarchy, and self-organization in a system help the system to function effectively (Mangal, 2013).

Complexity theory. Cairney (2012) gave new insight into the work of von Bertalanffy (1972) by introducing the complexity theory. In the complexity theory, Cairney highlighted the instability and disorder in politics and policy-making then links these factors to the behavior of complex systems. Cairney also suggested the political system should no longer be analyzed by segmentation, but as a whole system; furthermore, by taking such a stance, the result of interacting and combining networks will produce dynamic behavior.

The approach of the complexity theory provides a view of the organizations as a complex adaptive system that allows management to make strategic and operative decisions by reducing the complexity of the volume of information flowing through (Basile, Kaufmann, & Savastano, 2018). Basile et al. (2018) further indicated when an organization is in a turbulent environment; management must introduce a variety of competence and strategic intelligence to manage the dynamics of the situation successfully. The complexity theory is a relatively new school of thought and is complimentary of evolutionary theories of adaptation (Cairney, 2012); furthermore, it is closely related to the chaos theory per the focus on effective management during a disruptive event.

Chaos theory. Cyber events are increasingly common, and when an organization has been affected, there can be a significant financial cost including legal liabilities, damage to the brand, regaining operations, sales, and customer trust (Gwebu, Wang, & Wang, 2018). It is pertinent for managers to develop preventive maintenance around planning and mitigation of these events. The chaos theory as developed by Burns (2016) is a belief that external forces can influence important decisions and can cause much disruption within an organization, substantiating the importance of effective management during a cyber event. It is the role of management to effectively manage the moving parts and collaborate with IT administrators regarding identifying control and security failures, conducting forensic investigation, restoring operation and security, preventing possible repeated attacks, and determining when and what to communicate with senior executives, business functions, legal counsel, and the public relations function, and even more, the organization.

It is essential for management to engage in delivering a comprehensive understanding of the situation, and that can be achieved through updating. Updating during a crisis allows individuals to modify the course of action based on new information; it also allows emerging problems to be noticed and resolved (Christianson, 2019). Management should ensure the identification of the root cause of the event because if the situation is ongoing, the organization could remain in a state of confusion and deeper financial loss. Dependable security in an organization starts at the top and not with firewalls or biometrics; it begins with senior management.

***Multilayer security theory*.** When an organization is involved in a cyberattack, Lee and Kang (2015) brought forth the concept that several techniques rather than a single technique would be a more effective strategy to block the attack. Their theory is that a multilayer security scheme defends against diverse types of cyberattacks in a systematic and adaptive approach. More services require more computers that are interconnected, providing more information that must be transferred over these networks.

Multilayering is a concept that is a cornerstone of aviation security. The school of thought is one layer has the ability to compensate for the limitations of another layer; therefore, a strong defense has been created to deter an attack or produce a failed attempt of an attack (Jackson & LaTourrette, 2015). Insights from an analysis of safety systems suggest multilayers have the propensity to undermine one another; however, Jackson and LaTourrette (2015) advised that layers provide greater protection together than the sum of their individual effects.

Production theory. One of the major issues that burden the airline industry is how to allocate scarce resources efficiently enough to reduce the probability of a cyberattack. The production theory pertains to trade-offs between different inputs in the production of airline security. An example of this theory would be how the technology of production relates to factors such as labor, or capital equipment are combined to produce clearly identified outputs; thus, establishing that within a given technology of production, the same level of production can be created using a variety of combination inputs (Gillen & Morrison, 2015). For further discussion, individuals must determine if a level of airline security is obtained through labor- or capital-intensive form or via a balanced combination. The more efficient means of production may depend on the relative output and cost of each point.

Contrasting theories. Christensen, Baumann, and Sadtler (2006) introduced the idea of catalytic innovation, which challenges industry incumbents by offering simpler alternatives that are distinguished by their primary focus on social change. Also, in contrast to the general systems theory of von Bertalanffy (1972) are Christensen, Raynor, and McDonald (2015) who described the disruptive theory as circumstances where technology/innovation is the victim of its success. Future study on this theory is needed; however, universally, it has been ignored. Empirical tests reveal disruptive theory provides an accurate insight but does not disclose everything about innovation and how to best meet the challenges of this phenomenon.

Fundamental concepts may include that many airline leaders are not aware of the devastation of cyberattacks or that it is a new form of warfare. Many scholars view cyberattacks as disruptive innovation, whereas, an industry may be shaken up and stumble; furthermore, when changes in an industry’s competitive pattern exist, distinct types of innovation require several types of strategic approaches (Christensen et al., 2015). Other concepts include that leaders ponder how to display resiliency once an attack has occurred. The accidental losses of information have resulted in 5,810 data breaches made public from 2005 to present (comprising some 847,807,830 records), and the velocity of these events is increasing (Brown, 2016).

Proper management of a breach response can reduce response costs and can serve to mitigate potential reputational losses. Brown (2016) theorized organizations must be prepared for a possible breach event to maintain cyber resiliency. It is the perfect coordination between the risk assessment mechanism, and the response system of the model would lead to an efficient framework. Brown believed such a model would manage risk reduction issues, calculate the response, and conduct response activation and deactivation. Per this theory, the system is examined from the point-of-view of the attacker.

Security and Prevention

Cyber-warfare may be described as the application of computer networks to disrupt, deny, degrade, or destroy information contained in alleged enemy computers and networks; thus, it is an emerging form of conflict, also referred to as offensive capabilities in cyber-space, with the intent to gain from the loss of others (Crespo, 2018). To further substantiate the probability of the growing phenomenon, Patterson (2015) believed because of high profile attacks, globally there is a realization of the need for expanded cybersecurity and the capability to be offensive, as cyber-war has become the new frontier on the battleground. Patterson also alluded to former President Obama, who declared the phenomenon as one of the most severe threats to public safety and economic stability. Technology continues to advance and causing a widening gap between risk and defense.

Abomhara and Køien (2015) defined security as a process implemented to protect objects against unauthorized access or loss by preserving the confidentiality and integrity of information about the matter. With data being the lifeline of organizations and of utmost importance, the ever-increasing trend in information breaches (cyberattacks) has led to enormous losses. The security of information system resources is paramount (Patterson, 2015). Vulnerability issues may be considered as having interconnected impacts because the communication channel of an organization may consist of network technology, such as the intranet, extranet, and Internet. In application to this study, IT administrators and managers in the airline industry, as well as other sectors may gain a heightened awareness regarding this problem with disruptive technology, specifically cyberattacks, and thus, possibly implement strategies to reduce the fiscal impact.

A Historical View of Cyberattacks

Findings indicated that hostile foreign intelligence agencies were already hacking into services when Ronald Reagan was president (Kaplan, 2016). Kaplan (2016) also stated during the presidency of Barack Obama, cyber-warfare escalated and came to be noted as one of the few sectors of the defense budget where an increase in funding was seen. There were daily reports of cyberattacks launched by China, Russia, Iran, Syria, North Korea, and others; furthermore, these attacks were not just launched against government entities. Banks, retailers, factories, electric power grids, waterworks, and in this case, the airline industry were also impacted.

The financial implications of cyberattacks will continue to grow because businesses are increasingly moving online and becoming more dependent on technology (Center for Strategic and International Studies, 2014). A summer 2015 outage, incurred by a major airline, raised concerns regarding computer resiliency and safety (Holt et al., 2016). The blackout was a reminder to all U.S. carriers and consumers of the growing dependence on technology and the problems faced when technology does not operate as designed. Hackers were able to steal data on flight manifests, corporate data, seat numbers departures, and other items (Holt et al., 2016). The company credits a faulty router for this issue, which led to 61 flights being canceled and 1,100 flights delayed. The data breach cost the carrier about $4.6 million (Fox, 2016). Cyber-criminals are the source of most computer outages, and their far-reaching ripple effects cause global problems.

The Three-Prongs of Cyber

McGraw (2013) identified the three challenges that generate fear, uncertainty, and doubt for IT and cybersecurity are cyber-war, cyberespionage, and cybercrime, with cybercrime being the most common. Cybercrime is a well-established phenomenon (Ablon & Libicki, 2015). Cybercrime is no longer a hobby, but it has become a lucrative economic venture and business (Kigerl, 2018).

Cybercrime. Hewes (2016) defined cybercrime as a criminal activity involving the Internet, a computer system, or computer technology and may include:

- Identity theft
- Phishing schemes
- Theft of corporate funds, assets, and computer resources
- Disclosure, modification, or destruction of personally identifiable information or proprietary information
- Abuse of computer resources for unauthorized purposes or to launch attacks on other systems
- Causing damage to networks and equipment

Hewes (2016) also provided statistics stating approximately 100,000 cyber incident reports were generated that detected 64,000 significant vulnerabilities, issued nearly 12,000 alerts or warnings, and responded to 115 significant cyber incidents in 2014 alone. It is not only big businesses being targeted as 60% of all targeted attacks struck small- and medium-sized organizations. Five out of every six large companies (2,500+ employees) were targeted with spear-phishing attacks in 2014, a 40% increase over the previous year; additionally, small- and medium-sized businesses also saw an uptick, with attacks increasing 26% and 30% (Hewes, 2016).

Cyberespionage. Cyberespionage, which is also known as spying technology, allows for a vast amount of information to be gathered by rummaging through a competitor's website for product, employee, and information; furthermore, enabling hackers to transcend beyond the limits of intelligence by engaging in illegal activity (Bressler & Bressler, 2015). The cost of corporate espionage appears to be approximately $100 billion per year and generating a 25% increase per year member increase in the Society of Competitive Intelligence Professionals (Bressler & Bressler, 2015). It is no difficult feat to transfer, store, and hide information, while more information than ever is stored and manipulated on networked machines (McGraw, 2013). To identify the behavior of cyberespionage can be problematic as some malware or malicious behavior may have a context that can be difficult to locate (Brantly, 2016). The advancement in technology has made cyberespionage more common than cyber-war and has made it easier to expose secrets.

Cyber-war. Cyber-war, cyberespionage, and cybercrime constitute a three-pronged cyber challenge with the same root cause, playing on the world's dependence on networked computer systems. McGraw (2013) defined cyber-war as a violent conflict between groups for political, economic, or ideological reasons. McGraw also shared the fact that hackers tend to draw much public attention and tend to infiltrate some systems to demonstrate their hacking prowess. Compromised information could include credit card information residing in point of sale terminals, designs of weapon systems, or the secret seeds to one-time password tokens. The act of cyberattacks can be traced back decades, and because every attacker has a vast set of tools available, there are many more types of advanced attacks than attackers.

The attacker could take the form of a cyber-criminal, hacktivist, insider, or national spy agency. Additionally, the attacker has usually already determined the targeted organization has information of use to them. Unfortunately, society has an increasing demand for the latest and greatest technology and makes security more of an afterthought, and this gives a hacker a head start. Through the implementation of new cyber laws and practical strategies, organizations' leaders could see a decline in the three-prongs of cyber.

The Influence of Management

The effect of management may be considered as views implemented per practices or policies of an organization. It is management that may be one of the most significant obstacles in preventing improvement in the quest for cyber resiliency; thus, a lack of managerial support may be a devastating factor (George, 2016). The world is changing; management theory should change as well. Society should embrace an awareness of the new and emergent phenomenon. An avenue suggested by Mossburg (2015) for impact is to study aspects in which society does not yet have an intuitive gestalt, such as cyber-warfare, because managers generally place their focus on budgets, productivity, and timelines, giving little to no attention to cyberinfrastructure. A practical managerial response could contribute to positive cash flow, competitive advantage, sustainability, and organizational growth. Management has a responsibility as a defender of the fiscal health and performance of companies, which is critical in protecting an organization's most valuable assets (Mossburg, 2015).

Aside from determining the voice of the organization during a crisis, management is often the first voice of the organization, understanding that a quick response is essential. Crisis plans should consider the board's role and how it may be appropriate for the board to be a voice in the dialogue with stakeholders. Although members of organizations expect the board of directors to protect them from cyberattacks, the directors are usually unprepared for this role; furthermore, 58% of the board members identify cyber-related risks as the most challenging risk they will oversee (Rothrock, Kaplan, & van der Oord, 2018). Without close communication between the board and management, the organization could be at even higher risk (Greene et al., 2017). As the board's role in cyber-risk oversight evolves, the importance of having a robust dialogue with management cannot be overestimated.

There has been growth in groups, organizations, and in national and international entities allowing them to become open systems in terms of information access, which gives way to the growth of different information available to society (van Knippenberg, Dahlander, Haas, & George, 2015). Attention to prevention or cybersecurity should not just be a priority when an organization's interests, financial and otherwise, have been attacked. The role of management personnel should include placing focus on the creation of guidelines that affect policies and procedures involving cyberinfrastructure. Management must make a shift from placing so much focus on the IT department and focus on the entire organization (Rothrock et al., 2018). Shaw, Bansal, and Gruber (2017) suggested the need for management to embrace the newer side of the continuum and release the sedative of the ordinary. Also, management should invest in IT personnel who can seek to understand the behavior patterns established by hackers, develop safeguards, implement practices to help careless employees avoid providing hackers with access to the system, and introduce new computer systems.

The airline industry is struggling with aging technology, regulations, and a complex web of computer systems. Gillen and Morrison (2015) claimed that the systems are so layered on top of each other that it is difficult to tell who is talking to whom and a systems upgrade could cost one carrier $75 million. Declining profits are a factor for the airline industry based on rising fuel costs and consumer demand. Another roadblock cited by Gillen and Morrison is that management has a concern that the systems run 24 hours a day, 365 days a year, which makes it difficult for a carrier to cease operations for about four days to install a new system. Global regulatory requirements also make it difficult for management to perform a full-scale overhaul. Sabillon, Cavaller, and Cano (2016) referred to a cybersecurity policy as an instrument developed by nations to communicate and express specific areas in need of state protection concerning cyberspace. Additionally, Sabillon et al. stated that the cybersecurity policy is a statement, which embraces the understanding that binds a government to citizens, their rights and duties that are in a phase of reality in a society where instant information, mobility, and social networks are the norms of its operation. A new challenge for sound science is regulation regarding a situation that is unpredictable, yet, there must be an attempt to conceptualize and propose solutions (Sabillon et al., 2016).

Reducing the fiscal impact of the cyber-phenomena should be the goal of every organization, institution, or government globally. Active engagement is limited because research is sparse (Ferdinand, 2015). Ferdinand (2015) shared that management should display resilience composed of a complex combination of system hardening, system defense, access control, risk management, physical security, procurement control, internal and external monitoring, and security training. Based on the results of this study, leaders may understand the need for strategic management through an organizational commitment to prevention, protection, and a focused approach to cyberattacks. There exist some federal statutes of which Hewes (2016) urged managers to be aware:

- The Electronic Communications Privacy Act of 1986, which amended the federal wiretap statute and made it illegal to intercept stored or transmitted electronic communications without authorization.
- The Wire Fraud Act 2010, which covers any fraudulent scheme to intentionally deprive another of property or honest services via mail or wire communication.
- The National Stolen Property Act, created in 1998, prohibits the interstate or international transportation of the proceeds of theft and certain types of forged securities.
- The Identity Theft and Assumption Deterrence Act of 1998, which makes identity theft a federal crime.
- The Privacy Act of 1974 established a code of fair information practices for individuals maintained in a system of records by federal agencies.

- The Digital Millennium Copyright Act implemented in 1998 and prohibited circumventing a technological measure designed to protect a copyright.
- The Cyber Security Enhancement Act of 2002 granted sweeping powers to law enforcement organizations and increased penalties imposed by the Computer Fraud and Abuse Act.
- The National Cyber Security Protection Act of 2014 placed within the Department of Homeland Security (DHS) the national cybersecurity and communications integration center. One of the primary duties of this center was to serve in the oversight of cybersecurity (Hewes, 2016).

Cyber-risk has become increasingly one of the major concerns for companies. The financial implications of a single event involving one major corporation in 2013 had an estimated range from $11 million to $4.9 billion (Wolff & Lehr, 2017). Two-thirds of the organizations that suffered cyberattacks incurred an adverse result on the share price. It is an essential task for boards to verify that management has a solid mindset of how the organization could be severely impacted, and that management is empowered with the proper skills, resources, and a plan of action in place to minimize the cyber-incident and to reduce any damages that could occur (Greene et al., 2017). There is a great need for management, inclusive of board members, to give as much concern to cyber resiliency as they do other operations.

Information Technology Personnel and System Administrators

There is a dire need for IT personnel because computing technologies offer many opportunities and complexities to which the casual user is oblivious. Traditional IT administrators have been known to function as technical centers, which provide support to the other units of an organization, however, in the digital era, their role is more to create new content and knowledge that affect positive social and environmental change (Hsu et al., 2018). IT personnel may provide the role of handling cybersecurity and information security. The terms cybersecurity and information security are used interchangeably, despite representing different aspects of security. Cybersecurity goes beyond the boundaries of traditional information security to include not only the protection of information resources but also that of other assets, including the person, while information security refers to the human factor and may relate to the role of humans in the security process. Additionally, the protection of an organization's information is an essential aspect of an organization and IT strategy. The importance of computer professionals includes (a) their general knowledge of computers and networks regarding cyberattacks, (b) their engagement in research and published findings, (c) the development and participation in cyberattack and defense exercises, (d) their involvement in groups and conferences focusing on the phenomenon and defense, and (e) their attention to computer system weaknesses and network vulnerabilities (Denning & Denning, 2010).

IT personnel may be viewed as experienced defenders (antivirus software developers) who are continually changing, and in doing so, are also delivering better means of blocking hackers with a virus immunity ecosystem (Mithas, Kude, & Whitaker, 2018). Computer viruses are very prevalent in society, which can promote the use of antivirus software, which may include firewalls, virtual private networks, and antispyware software by IT personnel. Mithas et al. (2018) stated computer viruses are evolving and becoming more complicated, unpredictable, and destructive; thus, malicious software is being revised to become more resistant to antivirus software. The more these experienced defenders learn about the resolution of malware, the more efficient they become in repairing vulnerabilities and preventing malware from infecting computer systems. At one time, hackers invented viruses for the sake of the bragging rights, and now hackers are mixing with fraudsters and organized crime rings (Hsu et al., 2018).

Roel Schouwenberg is a senior researcher for Kaspersky Lab, a leading computer security firm, who spends numerous hours fighting one of the most horrifying cyber weapons introduced, Stuxnet. Stuxnet has the ability to cripple infrastructures that were once thought to be impenetrable and was initially designed to cause an interruption in the Iranian nuclear program (Nourian & Madnick, 2018). Nourian and Madnick (2018) also advised this weapon is a highly sophisticated collection of malware, and a computer virus such as Stuxnet is dependent upon unsuspecting victims (such as the internal employee) to install it, then the worm spreads on its own, often covering an entire computer network. It is necessary that cybersecurity measures identify vulnerabilities, risks, and solutions.

Many employees lack the knowledge of what to do in the event of a cyberattack, which usually causes them to go in disarray wondering who is in charge and what should be done. If an organization has a good incident response plan, the roles and responsibilities of the teams involved are clearly defined. The groups may include crisis communications, human resources, legal, and of course, IT (Brown, 2016). Failure to organize could lead to not only financial devastation, but also increased data loss, exposure to regulatory action, and reputational damage.

The Internal Threat

Ironically, many hackers are mythically portrayed as perceptive programmers sitting in a dark room seeking vulnerability through computer codes or software. In actuality, internal factors too often grant access to hackers resulting in data breaches or cyberattacks. Rid and Buchanan (2015) defined attribution as the art of determining who committed the crime and is at the core of coercion and deterrence, international and domestic. Realizing the offender requires that uncertainty is to be minimized on three levels such as tactically, operationally, and strategically. For the organization to be successful in attribution, the employees must display a wide range of skills, effective management, time, leadership, stress-testing, practical communication skills, and the ability to recognize limitations and challenges (Rid & Buchanan, 2015).

Malicious insiders pose a significant threat to organizations, as they possess the knowledge and have access to an organization’s resources. It is these insiders who can launch attacks quickly and cause more damage compared to outsiders (Liang et al., 2016). A clear majority of the technology used is connected to a network and the Internet; therefore, organizations may become vulnerable to cyberattacks or data breaches because the points of entry may include employees, third-party partners, and even customers (Ablon & Libicki, 2015). Liang et al. (2016) wrote the internal attacks are not only easier to launch but also can be more devastating. One can expect to see a financial loss, organizational disruption, loss of reputation, and a long-term affect on the organizational culture when a malicious insider has launched an attack.

There are many reasons that otherwise, ordinary employees may become an internal threat. One such idea is ethical issues, as mentioned by Chatterjee, Sarker, and Valacich (2015), which may be identified as a lack of empathy or conscience. The malicious insider lacks integrity and experiences no remorse for the harm imposed on others, and in an improper manner. The Centre for the Protection of National Infrastructure (CPNI, 2013), advised issues may also include reduced loyalty or diminished attachment to the organization.

Employee fraud, which is one type of malicious attack, has also been aligned with ethical flexibility. Insiders may suffer social isolation problems such as chronic problems getting along and working with others. Malicious insiders may display the characteristics of being an introvert, may appear to be overly dependent on computers, and may experience stressful work-related events such as sanctions or internal audits; however, it is the stressful experience of employees that tend to lead to a higher probability of security breach (Smrithy et al., 2018). Chatterjee et al. (2015) cited personal or emotional issues as a trigger for the malicious insider. The issues could include the loss of a family member, a relationship breakup, or significant personal injury, suggesting malicious insiders are emotionally unstable and might react to work-related issues negatively instead of constructively. The insider may develop a sense of feeling betrayed, isolated, exclusion, thus, resulting in a show of anger, poor attitude, or stress. Some researchers stated that instead of feeling negative, malicious insiders might seek sensation as an emotional response as many studies indicated malicious insiders are also disgruntled employees, and the disgruntlement might be a result of unmet expectations, lack of appreciation, and feelings of injustice or inequality (Voris, Song, Salem, Hershkop, & Stolfo, 2018).

Social and cultural conflict may be defined as the difference in groups such as racial, social, or technical that leads to a conflict between the various groups and others. Malicious insiders are frustrated with their personal or social relations (Chatterjee et al., 2015). Chatterjee et al. (2015) suggested hackers often find their way through the best cyber defense technology by locating the weakest link, which is the human operator. They use tactics deemed as social engineering and spear-phishing to exploit unsuspecting employees and breach networks. Education is a viable defense in the cases mentioned previously.

Organizations, such as airlines, store data in so many areas that nearly every credit card transaction, whether online or in-person, increases the risk of a data breach. Cloud-based systems are now connecting everyday items such as refrigerators and telephones, which also increases the risk of a data breach (Smrithy et al., 2018). The ability to share information through such devices, such as fitness data from a Fitbit or even business to business information, places individuals and organizations at risk to be compromised. Many companies have fallen prey to corporate espionage or malicious insiders who seek financial gain by selling or stealing the organizations’ intellectual property.

In 2015, a security researcher tweeted about the ability to control the aircraft of a major U.S. carrier (Fox, 2016). It was reported the hacker claimed to have gotten into the control system aboard the airline about 20 times by using an ethernet cable that had been modified and connected to a laptop, then to an electrical box under the seat on the plane. The hacker claimed to have demonstrated the ability to cause the airplane to climb or fly in a lateral movement. The hacker was arrested while exiting the plane after officials observed Twitter posts that the individual had made while in-flight (Fox, 2016). Ellis and Marco (2017) discussed an incident that occurred on January 22, 2017; a computer problem temporarily grounded all domestic mainline flights. The flights were grounded due to a problem with the communication system that airplanes use to send information to their operations. Situations of this nature are usually controlled using the Aircraft Communications Addressing and Reporting System (ACARS). The purpose of ACARS is to record and transmit a range of information, including departure times, as well as weight and balance, which is used to calculate takeoff speeds (Ellis & Marco, 2017). Confidential information is best stored in areas where access can be adequately controlled. A data security program is essential for diminishing various threats and avoiding data rupturing. By having a security plan in place and practicing it regularly, organizations will notice a decrease in exposure to risks and an improvement in the overall safety of data.

Financial Implications

The topic of cybersecurity must be brought to the forefront by financial institutions and the threats addressed holistically by management. The need for security and intensified commitment to providing it reveals new threats and vulnerabilities daily; thus, businesses continue to incur sizable financial losses because of security breaches (Ring, 2015). A small percentage of CEOs realize that the actual cost of cybercrime and that it stems from delayed or lost technological innovation problems resulting in part from how thoroughly companies are screening technology investments for their potential impact on the cyber-risk profile (Khan, 2019). Khan (2019) also advised many organizations face difficulty in quantifying the effects of risks and mitigation plans without realizing much of the damage results from an inadequate response to a breach rather than the violation itself. Managers need to understand the effects of cybercrimes on an organization vary, and so should the answers to them.

Among the many identifiable threats, computer viruses rank as one of the most serious in terms of their affect and frequency. There are many economic calculations, and although they may vary, cybercrime, combined with data loss, has an estimated global loss of at least 1 trillion dollars annually (McGraw, 2013). The annual cost for businesses worldwide is approximately $400 billion (Braunberg, Walder, & Spanbauer, 2014).

Horowitz (2012) developed a theory regarding the diffusion of new military capabilities known as adoption capacity theory, which illustrates cyber weapons are likely to spread quickly. Adoption capacity theory was based on the thought that the diffusion of military innovations depends on two intervening variables: the financial intensity involved in adopting the capability and the internal organizational capacity to accommodate any necessary changes in recruiting, training, or operations to embrace the ability. The low financial and regulatory barriers to developing cyber-warfare capabilities indicate the adoption of cyber warfare will be widespread. Mossburg (2015) introduced a study that has brought deep insight into the financial impact of cyberattacks as the researcher describes operational destruction and organizational disruption as far more impactful than the attack. Mossburg continued to explain direct costs, which are associated with customer notification, post-breach assurance programs, regulatory fines, public relations, technical analysis and remediation, and litigation.

It is crucial for risk officers to realize the threat of cyberattacks and to respond with budget allocations, reliable IT security programs, and cyber-insurance; however, if no cyber-risk program exists, this can leave an organization unknowingly exposed to even devastating financial consequences. Mossburg (2015) identified the financial implications and its effects as (a) closer compliance scrutiny, (b) higher cyber-insurance premiums, (c) waves of public relations and legal costs, (d) increased cost to raise debt-cyberattacks, (e) a downgrade of this nature could cause a company an additional $3.6 million in interest over the lifespan of a $100 million project, and (f) affects on customer retention cost of sales, and revenue.

It is pertinent for organizational leaders to gain a clear understanding of the fiscal implications that can be caused by cyberattacks. Hewes (2016) explained such an opinion could be useful in helping organizations to calibrate their levels of investment; furthermore, boards should accept the responsibility of understanding how management determine what investments to make and how to allocate resources that will monitor cyber-risks, as well as guard against it, and accelerate the process of response and recovery. Regardless of how effective a company’s outward defenses are, if no preparations have been made to respond to the breach, the company will suffer severe damage. As the concern regarding the financial implications of the phenomena increases, so does the need for a heightened awareness from management.

Strategies to Reduce the Fiscal Impact of Cyberattacks

Disappearing are the days when companies sought coverage from general liability or business owner's policies for coverage; however, it can be challenging to find the right coverage because of a lack of consistency being offered by insurers. Mossburg (2015) suggested leaders consider the function of insurance and implement it into their cyber-risk program; additionally, cyber-insurance is a new market, and in 2017, Americans spent $4 billion purchasing the insurance. That number is expected to increase to $9 billion by 2020 (Kshetri, 2018). A study by Zureich and Graebe (2015) indicated the average cost paid by organizations for data breaches increased from $5.4 million in 2013 to $5.9 million in 2014, causing specific cyber-insurance policies to grow in popularity and to become a strategy that should be given thoughtful consideration. Cyber-insurance can be a robust market, as in 2013, the entire U.S. cybersecurity market when measured by gross written premiums, was only $1.3 billion (Braunberg et al., 2014). Zureich and Graebe identified first-and third-party coverage, whereby, first-party coverage includes insurance for losses to the policyholder's data or lost income, or for other harm to the policyholder's business resulting from a data breach or cyberattack. First-party coverage is as follows:

- Theft and fraud - This coverage provide for the destruction or loss, and unlike most insurance companies, it is inclusive of theft and fund transfers.

- Business interruption - Coverage of lost income and related costs when a policyholder is unable to conduct business due to an event.
- Extortion - Ensures values that have been acquired with investigations related to threats against the policyholder's systems and for payment to extortionists.
- Computer data loss and restoration - Relates to the coverage of physical damage and the costs of retrieving and restoring data, hardware, and software or other information destroyed or damaged by a cyberattack.
- Security breach remediation and notification costs - Covers the costs to identify who was concerned, notify customers, employees, or other victims affected, legal expenses, and credit monitoring.
- Crisis management - Covers crisis management and public relations (Zureich & Graebe, 2015).

Third-party coverage, as defined by Zureich and Graebe (2015), covers the liability of the insured to third parties arising from data breach or cyberattack. Typical third-party coverages may include network and information security liability, regulatory response, and communications and media liability. Cyberattacks, even data breaches, can be devastating to an organization; however, specialized cyber liability insurance coverage can ease the burden. The market for this insurance is very fluid, and the available coverages vary immensely (Zureich & Graebe, 2015). Organizations now have a wide selection of underwriting companies from which to choose.

Cyber resiliency. To achieve the function of becoming cyber resilient, incident preparedness is of vital importance. Brown (2016) conducted a study which indicated

92% of those surveyed believed cyber-risks pose a moderate threat to their organization and some in senior leadership roles are disinclined to address cyber-risks; additionally, Brown indicated 68% of board members now believe cyber-risks pose a significant threat to their organizations. This attention is the reason senior leaders have begun to consider cyber-risk as a material threat, and a greater focus has been placed on being proactive to minimize exposures.

Too many organizations believe robust defenses will protect them from attack, and these same organizations fail to prepare for when the offense does occur. Research by Huang et al. (2018) indicated cyber events are such a phenomenon in the digital society that the estimated cost will increase from $3 trillion in 2015 to $6 trillion by the year of 2021. The threat should be rigorously countered at every single stage. By doing so, the identified attack will be responded to sooner allowing response procedures to kick in, isolating the attack surface, quarantining systems, and preserving security for areas unaffected (Brown, 2016).

Engaging people. An effective strategy should include process, people, and planning. Education is a critical strategy to reduce the fiscal impact of cyberattacks because employees should understand the importance of protecting data belonging to the company and its customers (Huang et al., 2018). Huang et al. (2018) also suggested organizations should implement attack-type exercises to build institutional capacity muscle memory. Another aspect of organizational engagement would be pre-planning through group input. Hall (2016) stated thieves are experienced, and they have a plan of action; consequently, leaders of organizations should properly engage people to battle the attackers by turning what may be deemed as a weakness, into a strength. Cybersecurity should no longer be viewed as the responsibility of the IT department only.

Secure software. There are vast opportunities for an attack in the cyber-environment. One of the best solutions to protect cyber defenses is to design and implement secure software to correct the broken systems first (McGraw, 2013). If organizations fail to achieve their competitive intelligence departments and consultants, such actions suggest corporate espionage to be a significant problem facing corporate America (Bressler & Bressler, 2015). Ben-Asher and Gonzalez (2015) developed a simplified intrusion detection system (IDS) in their efforts to examine how individuals with or without knowledge in cybersecurity detect malicious events and determine if the intrusion is a justified attack based on a sequence of network events. Ben-Asher and Gonzalez developed a strategy leading to the indication that more knowledge in cybersecurity facilitated the accurate detection of malicious activities and decreased the false classification of benign events as malicious. Understanding of cybersecurity helps in the discovery of malicious incidents; however, situated learning regarding a specific network at hand is needed to make accurate detection decisions (Ben-Asher & Gonzalez, 2015). Also, there must be the collaboration between executives and members of the organization.

For organizational leaders to be resilient, they must ask themselves about the effectiveness of the security controls they have in place. In this regard, Braunberg et al. (2014) wrote if an organization is susceptible to an attack from Java exploit, but the intrusion prevention system (IPS) deployed has the capability of identifying and blocking the exploit, the organization is protected and not at immediate risk. The focus of organizations should deflect from the 98.5% of attacks being detected by the security controls already in place, but emphasis should be directed to the 1.5% of attacks that travel unnoticed through existing defenses; in addition, attention should be placed on whether those missed attacks are relevant to the organization (Braunberg et al., 2014). The information shared here supports the general systems theory (von Bertalanffy, 1972) that to resolve the problem, organizations must review the system as a whole.

Response plans. Incident response plans (IRP) should be a primary priority, and at the forefront of every organizational leader's mind, however, numerous organizations are still in the process of developing response guidelines. An IRP, as described by R. Collier (2016), established the various phases necessary or an outlined strategy to protect personnel, incident assessment, protection and retrieval of information, and any situations that may have been disrupted by the event. Brown (2016) estimated 72% of organizations have an established plan to reduce the potential cost affiliated with crisis management, reputation damages, and the loss of business interruption. R. Collier identified six steps as essential to conducting a prosperous IRP inclusive of preparation, identification, containment, eradication, recovery, and lessons learned. An effective response plan could be vital to an organization reducing the fiscal impact of a cyber event. Once an organization has created a data breach response plan, this can assist in minimizing the risks, costs, and devastation of the phenomenon.

Organizational leaders should understand the need to addressing the problem of cyberattacks with an intense refocus on energy, as opposed to building faster and more intelligent systems (McGraw, 2013). Leaders should be able to remedy the software security issue by identifying, understanding, and mitigating the risks and should conduct external scans frequently to detect vulnerabilities and patch the observed vulnerabilities because this is one of the best strategies for defense (McGraw, 2013). Additionally, by requiring a firewall and other guards protecting Internet-facing assets, this may be discouraging to a hacker because he or she does not have easily exploited vulnerabilities.

There is a new capability in threat management called security analytics (SA). Lino, Rocha, Macedo, and Sizo (2019) explained the fact that SIEM data and network traffic is examined, parsed, and analyzed to recognize when an attack is underway. When SA was first introduced, practitioners had to use labor-intensive tools to do these functions, but new programs like Prelert, Structured Query Language (SQL), and Lightcyber have automated the process. SQL may contain a wide variety of criteria that can identify which rows the user wants to retrieve (Lino et al., 2019). Consequently, as organizations are steadily utilizing novel technologies, the strategies for infiltration into systems are continually changing and becoming sophisticated. Cybersecurity activities should also consistently change and should no longer be confined to IT administrators. Cybersecurity should also include employee engagement.

Management has a responsibility to work with directors to develop a dashboard, which identifies the parts of the business with the greatest and least amounts of cyber exposure and the initiatives in place to reduce risks. Greene et al. (2017) stated boards of directors need useful metrics and analytics to gauge whether the organization is managing cyber risk at an acceptable level. Boards can also ask management about their use of risksensing tools. By practicing cyberattack simulations and other wargaming exercises, organizations can identify vulnerabilities and gaps in preparedness and improve the ability of management teams to make decisions under stress. Leading organizations involve management directly in such exercises, and it has been suggested board members are also included (Greene et al., 2017). The correlating theory of security decay is applicable as boards and management were included because Coole and Brooks (2014) supported the holistic approach.

As the Internet becomes more established, so does the opportunity for threats. The Internet of Things (IOT) security exceeds home environment monitors. IOT exceeds refrigerators that can order fresh milk and is causing a widening gap in the need for skilled workers and those able to fill the gap. The introduction of IOT has brought with it the possibility of closing the information gap. The use of IOT allows data to be delivered timely, accurately, and provides a high-quality information base. As a result of the reasons mentioned above, researchers have been applying IOT to various environments based on their expertise or experience (Qu et al., 2017).

IOT enables a connection between networks and objects that we use daily; furthermore, the use of IOT adds to society’s dependence on technology so much that areas of popularity range from entertainment to health care. This new technology brings a lot of valuable advantages and opportunities, but also many challenges, among which is hacking of personal devices (Zubiaga, Procter, & Maple, 2018). It has been projected that by 2020, IOT will be fully functional and 26 billion people will be connected to Internet-enabled devices; thus, only one entry to one tool provides the opportunity for a cyber-criminal to gain access to all machines on that server (Hall, 2016). There is no immediate sign of measures that would effectively address the complexity of IOT, which allows a continued opportunity for cyber-criminals.

Also new to the world of technology is artificial intelligence (AI). AI is also known as machine intelligence because it is a machine-learning algorithm. This machine intelligence could have a positive outcome globally, yet, it can cause severe social and ethical issues (Grosz & Stone, 2018). AI systems could effectively collaborate with humans and because of ties with large datasets, robotics, computers, and language systems. AI is a prime target for being hacked. The social media theory is one I considered when discussing IOT and AI because the theory states elements should interact with each other and with entities within the system to achieve a function as a whole; additionally, the information security elements should include collaboration and integration to minimize threats. When the appropriate segments are present, the system will function effectively, despite the fact the system may have to operate for an extended period.

There has been an influx of individuals entering cybersecurity careers because of a concerted campaign by the industry promoting awareness. Mithas et al. (2018) shared there is still a shortage, and by 2019, 6 million professionals will be needed; however, the projected number is currently only 4.5 million. This issue to be noted as the most substantial human capital shortage in the world. Without the appropriate workforce globally, companies will be unable to keep up with the industry and develop efficient technology and infrastructure to handle the new cyber-threats. Mithas et al. predicted that

AI could be the cause of a reduction in the workforce in general, but by 70% for software developers in India, which accounts for 65% of global IT offshore work and 40% of IT-enabled business process work. There is more of a chance the programming occupation will become extinct than it will become more powerful because of AI (Mithas et al., 2018). Organizations and industries alike must create specific strategies to increase awareness not only in the United States but in the global population also so that all are aware of how to protect themselves when using technology from the office to social media and smartphones.

Role of Cyber Laws and the Possible Fiscal Impact

The world has been faced with a plethora of traditional and non-traditional security challenges and is not equipped with proper services, information, and resources. For this reason, the need for cooperation between the public and private sector to establish democratic control policies regarding cybersecurity is clear (Spalević, 2014). While the various strategies as aforementioned are of excellent value, their effectiveness could be enhanced with laws to support them. In 2015, President Barack Obama signed into law an Executive Order that allowed government officials to confront malicious cyber activities by imposing sanctions on responsible foreign individuals and entities (Melnik, 2015). Melnik (2015) further discussed Executive Order 136942, which was designed to financially target and prevent malicious parties from practicing and profiting from cyber activities. Belli and Venturini (2016) advised U.S. representatives introduced more than 40 bills and resolutions with provisions relating to cybersecurity and Congress has not submitted a major proposal regarding cybersecurity to the President since about

2008; yet, the challenge continues to grow. Even though new legislation is needed, several acts that were created to affect the cyber phenomenon significantly include:

- The Federal Information Security Management (FISM) Act of 2002 requires federal agencies to assess vulnerability and penetration. It also allows the use of constant monitoring to detect, report, respond, contain, and tranquilize incidents. Additional requirements have been reviewed and would cost agencies a total of $150 million a year; unfortunately, no new funds are authorized (Francis & Ginsberg, 2016).
- The Cyber Intelligence Sharing & Protection Act (CISPA) is the most comprehensive of this bi-partisan bill, which passed House vote in 2012 and 2013, but the Senate has refused to implement it because they deem the act as lacking enough privacy protections. This bill would provide criminal and civil immunity for private sector security efforts and would promote better sharing by the U.S. intelligence community. It also provides 11 substantial amendments targeted at addressing any concerns (Schackelford, 2016).
- The Cybersecurity Act offers a provision that allows a private sector entity to operate, or approve the operation of, countermeasures that may be modified, redirected, or used to block information. Some deem the bill as vague, leading to The Cybersecurity Enhancement Act passed by the House. This act requires additional research into access control management, systems assurance, industrial control systems security, and supply chain management (Tran, 2015).

- The Computer Fraud and Abuse Act (CFAA) was enacted to address computer fraud laws already in existence. The primary purpose of this act is to prohibit individuals from accessing computers without proper authorization. Some leaders of organizations consider this law as ineffective (Simmons, 2016).

Bipartisan leadership and their staff are educated and active, but unfortunately, a solution to the matter has not been achieved. Additional areas of legislative focus include government procurement, workforce development, promoting international norms, and fostering public/private collaboration (Belli & Venturini, 2016).

Policymakers are experienced with numerous crises, yet, their understanding of the cyber phenomenon maybe with some exceptions and vague, even more so, politicians tend to have a reluctance to commit to some interpretations of cyber and to express their cyber opinion (Macak, 2017). For this reason, the role of IT personnel or computer scientist is also one of immense importance in helping to shape national and international policies regarding the cyber phenomenon. On a national issue, the balance between privacy and security has become an emerging issue, which indicates that there must be a modification of laws and practices in the United States on cybersecurity.

Transition

In Section 1, I provided insight into the specific problem some airline managers and IT administrators lack effective strategies to reduce the financial impact caused by cyberattacks. Also, in this section, I underscored the need for IT personnel to practice resiliency in terms of cybersecurity and I provided insight regarding the problem and purpose statements, nature of study, assumptions, limitation, and delimitations, research questions, and the conceptual framework.

In summary, cyberattacks can cause extreme financial devastation; thus, organizational leaders must have strategies of resiliency in places such as engaging the employees through process and planning, secure software, cyber-insurance, and laws. Organizations must also be aware of internal threats. Whether the breach has been implemented through cyber-war, cyberespionage, or cybercrime, statistics provided by Hewes (2016) shared that about 100,000 cyber incidents were reported in 2016 and the phenomenon is not isolated to large organizations.

In the event society is changing, the theories and awareness of management should change with it (George, 2016). Management should move beyond the details of productivity, budgets, and timelines, and focus on the emergent phenomenon of cyberattacks. Management should become more proactive in risk management, developing human defenses and a response plan through incident practice, and involving the board. By a similar indication, IT administrators should engage in research, develop and participate in cyberattack defense exercises, and participate in group discussions and conferences regarding the issue (Greene et al., 2017). Engaging the employees and an effective response plan are also pertinent.

In Section 2, I offer a synopsis of my role as a researcher, the participants, the technique and instrument used for data collection, the selected research method, design, sampling, and population. Section 2 also includes an overview of the reliability and validity of the study. The last segment of the study is Section 3. In this section is the presentation of findings, as well as recommendations for future research and implications for social change. As I provide my conclusion in this last segment, it also allowed an opportunity for personal reflections per my experience as a new researcher. By utilizing a qualitative single case study, I was able to understand strategies to reduce the fiscal effects of the phenomenon from the perspective of the participants. Also, I based my conceptual framework on the general systems theory of von Bertalanffy, which I found applicable to my research because I used airline managers from various departments to gather the whole perspective of their experience with cyber events.

Section 2: The Project

My intent for this study was to explore what strategies IT administrators and airline managers use to reduce the fiscal impact of cyberattacks. In Section 2, I explain my role as the researcher. I also share information on sampling, the participants, and eligibility requirements. Section 2 includes the research method and design, data collection, data organization, and information regarding ethics and instruments used for data collection. Section 2 also contains an analysis of the reliability and validity of the study.

Purpose Statement

The purpose of this qualitative single case study was to explore the strategies IT administrators and airline managers use to reduce the fiscal impact of cyberattacks. In this study, the population included IT administrators and management from one major U.S. airline who have used strategies to reduce the fiscal impact of cyberattacks. This study may contribute to positive social change by enhancing the knowledge of IT administrators, airline managers, and researchers. The implementation of enhanced knowledge could prompt legislators to understand the need for new cyber laws. With the passing of new and updated regulations, consumers, primarily in the airline industry, could benefit from the presence of a safe and secure environment. New regulations could bring the consumers comfort in knowing there is the protection of their personal information and transportation.

Role of the Researcher

My role as a qualitative researcher was to serve as the primary data collector. Per Rimando et al. (2015) the role of the researcher is to function as the instrument of qualitative research. My relationship with the topic extended from my experience as a former manager in the airline industry. Although the participants may have worked for the same organization, we did not have a direct relationship. Research participants are to be protected; thus, established values such as respect for persons, nonmaleficence, beneficence, and justice must be understood as guiding principles (Scherzinger & Bobbert, 2017). For this study, I followed the basic ethical principles to ensure the participants were comfortable and understood the process. *The Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research [NCPHSBBR], 1979) authors provided specific guidelines for ethical behavior. I conducted face-to-face and telephone semistructured interviews with the participants after clearly presenting and explaining the informed consent form.

My goal as the primary researcher was to mitigate bias and avoid a personal perspective. I reduced bias and avoided viewing data through a personal lens by asking the participants open-ended questions following an interview protocol as outlined (see Appendix). An interview protocol aligns the interview questions with the research and enhances the quality of the captured data (Castillo-Montoya, 2016). The use of an interview protocol also allowed me to conduct an effective inquiry-based interview and to receive feedback regarding the contract.

Participants

Eligibility criteria for study participants consisted of IT administrators and management personnel who have successfully used strategies to reduce the fiscal impact of a cyberattack and had a minimum of 5 years of experience. A primary characteristic of participants is they can provide accurate detail (Pham, Nguyen, & Chen, 2018). The participants were able to provide exact information because they have experienced the problem under study. Specifically, the participants for this study included members from IT leadership and members of the management team of one major U.S. airline. Organizational performance is usually improved by consideration of multiple perspectives and by adding administrators and managers from numerous areas (Lin & Chen, 2018). In this qualitative study, various perspectives were obtained until information became redundant.

I gained access to the participants via telephone, social media, and e-mail. My primary source of social media was via LinkedIn, an online public directory that allows a search by name, industry, or group affiliation. I established communication through Facebook. I used this mode of social media to open the lines of communication as part of my strategy for building a relationship with the participants to crate rapport before the actual interview. Perrin (2015) deemed social media as an effective method to connect with participants because the rise of social media has influenced nearly all areas of society and in some instances, the survival of organizations.

I conducted semistructured interviews that were face-to-face or via telephone. Ward, Gott, and Hoare (2015) shared that an assumption exists suggesting face-to-face is best for semistructured interviews. Ward et al. also concluded participants are more comfortable with the telephone interview. I further established a working relationship with the participants by carefully and thoroughly explaining my role, the goals of the study, and the purpose of the research, and by providing a comfortable and secure environment for the participants. I gave the participants individual identification codes ranging from P5-P11. I recorded, transcribed, and placed the responses on a spreadsheet for thematic coding. To enhance the credibility of this study, I used member checking. Member checking with the interview process provides the participants the opportunity to review the responses as well as confirm the information (Iivari, 2018). I asked the participants if they had public documents to share.

Research Method and Design

Research Method

The research method used in this study consisted of a qualitative analysis, which is a method of recording opinions, feelings, and experiences. This method was selected because it is the best form of research when a more in-depth understanding of attitudes, behavior, and motivations is required (Barnham, 2015). Qualitative data are impressive in the way the data are delivered because it may be digitized and synthesized. Qualitative data provide an interpretation of information that caters to insight and patterns (Pratima, Smith, & Vaara, 2018). The researcher must understand the participants’ biases have the possibility of influencing the results of the study (Clark & Vealé, 2018). I was the primary data collection instrument, and focus and interpretative thinking were critical for me and to better explain the topic.

Other methodologies used by researchers include the quantitative and mixed method approaches. Advances in technology have allowed researchers significant opportunities to access and analyze quantitative data and to obtain the results promptly from large numbers (Hochbein & Smeaton, 2018). Starr (2014) described quantitative research as the analysis of data using statistics. The research I conducted in this study did not require probability or statistics; therefore, the quantitative method would not have been an appropriate choice. Spoken or written language rather than numbers is data gathered in qualitative research. When spoken, the data are usually converted to text for analysis (Clark & Vealé, 2018). The qualitative method as described by Yin (2018) is a tool considered highly effective for exploring the reality of a phenomenon. Mixed methods combine the quantitative and qualitative analysis addressing the established research question. The use of mixed methods provides a more thorough perspective of the phenomena than the use of only one method (McCusker & Gunaydin, 2015). The mixed method approach was not appropriate for this study because there was no need for a quantitative component.

Research Design

In this study, I used a single case study design because the data collected was effective for analysis to answer the research question. Marshall and Rossman (2016) described the case study design as the allowance of an exploration of skills, knowledge, and strategies. The use of a case study design allows for the collection of several types of data, such as interview, observation, and document analysis. Researchers have the option to select from a broad range of designs (Yin, 2018).

There are several forms of qualitative designs of which researchers should be cognizant. Marshall and Rossman (2016) identified other qualitative designs as phenomenology, ethnography, and narrative research. Phenomenology is an exploration of the meaning of participants' lived experiences or phenomena (Lewis, 2015). A phenomenological design could have been used; however, I determined it as inappropriate for this study because my focus was more on the aspect of experiences related to technological skills.

The ethnographic design is one of the most respected forms of research. Ethnographic researchers focus on groups, organizations, or communities and their culture (Marshall & Rossman, 2016). In this design, strong emphasis is placed on the exploration of the phenomena because data are gathered from the participants' perspectives. Moreover, observation occurs in the participant's natural habitat of behavior and beliefs (Yin, 2018). The focus of this study extended beyond subcultures, which determined the use of ethnography was not applicable.

Narrative researchers explore the experiences of the individuals to formulate a robust chronological story (Beverland, Gemser, & Karpen, 2017). Beverland et al. (2017) also indicated a narrative design might be described as a conceptualization of multidimensional purposive communication from a teller to an audience. When using a narrative design, the researcher can expose people's values and personalities that may be derived from individual lives, circumstances, events, facts, behaviors, and experiences (Jordan, Bardill, Herd, & Grimaldi, 2017). The narrative design was also eliminated as a choice for this study because the focus is on strategies as opposed to life events. Fallan and Lees-Maffei (2016) identified narratives as having been criticized as outdated and static.

A researcher’s failure to obtain data saturation could interfere with the quality and validity of the study (Fusch & Ness, 2015). A researcher knows that data saturation has been reached when there is no additional information to be accumulated, and further coding is no longer necessary (Fusch & Ness, 2015). Saunders et al. (2018) stated there should be limits to the scope of data collection to prevent saturation from losing its coherency and the uses being stretched. I ensured data saturation by continuing data collection until there was no new information to extract.

Population and Sampling

The population from which the sample came included IT administrators and management from one major U.S. airline, who have used strategies to reduce the fiscal impact of cyberattacks. Purposeful sampling was used to identify participants within this population. Palinkas et al. (2015) described purposeful sampling as a method that is widely used by the qualitative researcher to aid in the identification and selection of studies that provide a wealth of information regarding the phenomenon of interest. Depending upon the various aspects of the population of the study, the sampling size has the propensity to differ (Solanki & Singh, 2015). Boddy (2016) advised when conducting qualitative research; the researcher must consider the sample size. According to Howes (2015), even fewer than five participants could be a sufficient number to provide perspectives that are relevant to a qualitative study.

Participants were included in this study whose primary responsibility included planning or responding to cyberattacks within one major U.S. airline. Specifically, the participants for this study included members from IT, as well as members of the management team of one major U.S. airline. Palinkas et al. (2015) indicated the selection of appropriate participants and sampling size is vital to a study because it provides a comprehensive analysis of the phenomenon. Malterud, Siersma, and Guassora (2015) stated when the research includes interviews, typically a sample size that is small, yet sufficient, is used, which allows individual participants to have a locatable voice within the study. It is possible as few as five participants could be a sufficient sample size to reach data saturation. Marshall and Rossman (2016) stated the effectiveness of the researcher in gauging the appropriate sample size has a direct correlation to data saturation. Data saturation may be defined as the process of introducing new participants into a study until the researcher completes the data set, which will be obtained when there is nothing new to add or redundancy exists (Marshall & Rossman, 2016). To ensure data saturation, I interviewed new participants until the information became redundant, and I had no further coding. During member checking, each participant was invited to validate or expand upon my analysis and summary.

Ethical Research

As part of ensuring ethical research, I e-mailed a consent form to the applicable participants after the Walden Institutional Review Board (IRB) approved planned research activities. By explaining and allowing the participant to view the consent form, the researcher can extend the discussion and provide a manner that is highly effective in helping the participants to understand their role in the study (Watts et al., 2016). Participants who were scheduled for a phone interview were asked to print, scan, and return the form with a signature indicating their consent. I reviewed and reconfirmed the consent form at the beginning of each interview, whether by phone or face-to-face. Chiumento, Khan, Rahman, and Frith (2015) stated the ultimate purpose of the consent form should be to protect the rights of the participants. Menikoff, Kaneshiro, and Pritchard (2017) expressed the researcher should ensure the consent form is clearly explained and understood by the participant and their participation is strictly voluntary. Participants were allowed the opportunity to withdraw from the study at any point in the research process by e-mailing me. It was also made clear in the consent form and in the interview itself that there are no penalties for withdrawing.

It was also made clear in the consent form no incentives for participation will be offered to the participants. It is safe to assume that individuals tend to participate in research studies because it provides a feeling that by doing so, they are benefitting humanity in general. Although related, ethics is different from laws, beliefs, religion, and attitudes. Ethics is a way of conduct and morality (Baral, 2016). The only benefits participants might extract from this study is the knowledge that by sharing their experiences, they are contributing to the expansion of knowledge on the topic.

I ensured the participants appropriate ethical protection is in place. I solemnly adhered to the basic ethic principles of the 1979 NCPHSBBR’s Belmont Report that promoted the researcher ensures the participants are comfortable and understand the process through the guidelines of respect of the person, beneficence, and justice. I also used a researcher’s journal and interview protocol.

Data will be maintained securely by storing all audio-recordings on an encrypted drive and securely kept in a locked file cabinet in my business office. The researcher is the only one with access to the file cabinet. Data will be kept for at least 5 years then destroyed.

It is the ethical duty of the researcher to protect the general welfare of participants (Wallace & Sheldon, 2015). No data was collected until Walden’s IRB provided approval. The IRB approval number for this study is 01-03-19-0169218. Killawi et al. (2014) promoted the protection of participants and their identifiable information. Personal information belonging to the participants were not shared in this story. Details that might identify participants, such as the location of the study, also have not been shared. Yin (2018) suggested unique identifiers to protect the confidentiality of the participants. I will not use the participants’ personal information for any purpose outside of this research project. Participants in this study are identified with a number between five and 11, as I did not use the names of the participants.

Data Collection Instruments

In this study, as the researcher, I was the primary data collection instrument through face-to-face and telephonic semistructured interviews and public document review. The instrument selection is of vital importance in the research process because the validity of the study depends on the instruments selected; furthermore, the ability to generate the same result consistently after multiple tests on the same group depicts the research instrument as reliable. Data collection instruments encompass the tools used for data collection and may include a questionnaire, interview, or observation, and the researcher must question if the interview questions will add to the existing literature. (Henderson, 2018). Seven open-ended interview questions were proposed to IT administrators and airline managers. I also used (public) document review to enhance and support data collected in the semistructured interviews. Participants were asked to provide related public documents, which could include policies, training information, news articles, or reports.

The document review consisted of public documents that were provided by several participants. The use of documents allows a researcher the opportunity to gain more insight into the subject matter and enhance understanding of the topic (Siegner, Hagerman, & Kozak, 2018). Yin (2018) mentioned various methods of data collection inclusive of interviews, digital recording, note-taking, observation, and peer-examination, which are highly successful in qualitative research.

I enhanced the reliability and validity of the information by using a member check process. Yin (2018) stated member checking could provide a more in-depth understanding. I used member checking as a method of exploring the credibility of the data. My interpretations of the participants’ responses were given back to the participants to review for accuracy. Birt, Scott, Cavers, Campbell, and Walter (2016) labeled trustworthiness as the bedrock of quality research. After asking the interview questions, I reviewed the responses with the participant for accuracy. Each participant was invited to validate or expand upon my analysis and summary. Several interview questions and protocol have been included in the Appendix.

Data Collection Technique

For this proposed qualitative single case study, I conducted semistructured interviews using an interview protocol (see Appendix) combined with member checking. Iivari (2018) stated the participants should be allowed to be engaged in the research process through confirmation and summation of responses to the interview questions. Asking the same questions in a sequential order allows the researcher to gather data efficiently and to obtain a better response comparison; furthermore, collecting data using more than one method enables the researcher to view the phenomenon from different angles and heighten the validity (Iivari, 2018). Multiple data sources provide an adequate snapshot of the real-life experience. I did request the participants share any public documents for review.

Semistructured Interviews

The first point of data collection for this study was semistructured interviews. Participants were first contacted either by phone, e-mail or over social media to determine the level of interest in participating. Once participants expressed an interest in participating in this study, a consent form was sent to them along with several dates and times to choose from for the interview. The participants chose between telephonic or face-to-face interviews based on their location and availability. Regardless of the mode of communication, the conversation began with a review of the consent form, a reminder that the participant can withdraw at any time and I provided them with the assurance I would follow the interview protocol (see Appendix).

The participants were also reassured of confidentiality and privacy. Carcone, Tokarz, and Ruocco (2015) advised there is strong support based on the reliability resulting from semistructured interviews; however, the validity of the semistructured interview is questionable. In qualitative research, interviews are one of the most common forms of data collection and require those specific standards are practiced, such as recording, archiving, and reinforcing the data (Rosenthal, 2016). After the semistructured interview, the participants were asked to share any documents that relate to the topic for a document review.

There are several advantages to semistructured interviews; Marshall and Rossman (2016) found semistructured interviews are the single best way to glean data in qualitative studies. Yin (2018) stated the use of semistructured interviews allow a researcher to focus on a narrow topic, which is another advantage. One disadvantage of semistructured interviews is the quality of data collected is dependent on the abilities of the researcher (Yin, 2018).

Document Review

Document review is the use of existing information on a topic that can provide a more in-depth understanding (Yin, 2018). Once the semistructured interviews were completed, the participants were asked to provide any related documentation, which could include policies, training information, or reports (public documents). The documents were reviewed, coded, and the data were combined with data from the semistructured interviews to present a robust, multidimensional look at how airline IT administrators and managers use strategies to reduce the effects of cyberattacks. The advantage of document review is the information can be expanded and support data collected in other ways (Yin, 2018). The major disadvantage of document review is the documents that could prove to be most helpful might not be accessible (Yin, 2018). Considering this proposed study is exploring the sensitive topic of cybersecurity, many documents that could have been helpful were not available for review due to security concerns while some public documents were made available.

Data Saturation

Data saturation applies to qualitative research that takes advantage of interviews as the primary source of data (Marshall & Rossman, 2016). I ensured data saturation by continually introducing new participants into the study until there was no new data and I reached a point of redundancy; consequently, there was no new coding, and I had acquired sufficient data for credible analysis. Researchers should discontinue the interviewing process when the participants cease to provide additional information regarding the topic for data saturation (Lowe, Norris, Farris, & Babbage, 2018). Lowe et al. (2018) further explained the researcher had reached the goal of data saturation when interviews with the participants yield no new emerging themes; furthermore, the responses are sufficient to justify the claims and conclusions.

Data Organization Technique

It can be expected every researcher has a traditional technique for remembering the details of an interview. I kept track of data through a researcher’s journal and a coding/labeling system. The data collected were coded by color. Slota and Madduri (2015) defined color coding as a technique that gives fixed-parameter tractable algorithms. Lauer, Brumberger, and Beveridge (2018) indicated data collection is of great importance in considering what research items could be replicated and could enable the researcher to identify patterns over time. Data from audio-recordings (digital files and the corresponding transcripts) will be retained for a minimum of 5 years and has been stored on an encrypted drive in a locked file cabinet. All data and related printed material that has been stored in a locked file cabinet and will be destroyed after 5 years. Additionally, any information shared via a social media tool will be deleted.

Data Analysis

For this study, I used the 5-step process introduced by Yin (2018) to conduct qualitative data analysis. The steps include compiling, disassembling, reassembling, interpreting, and concluding (Yin, 2018). By following this process, I was able to encompass various techniques. Data analysis may be viewed as an umbrella term that allows the researcher the ability to describe, decode, and translate, thus, revealing a clear understanding of the meaning (Mayer, 2015). Wahyudi, Kuk, and Janssen (2018) suggested the establishment of process patterns because they allow the researcher to implement a recurring sequence of steps that assist in obtaining goals.

To lessen the chance of biases while increasing validity, I used varying perspectives for this study. Joslin and Müller (2016) related the effective use of triangulation as identifying a person’s position by comparing the individual’s perspective to two other views. The use of multiple techniques enabled me to define themes and ultimately, strategies that may be implemented to reduce the fiscal impact of the phenomena. I used a single case study for this research. Yazan (2015) shared that a case study is an empirical inquiry and addresses the *how* and *why* concerning the phenomenon. My main goal as the researcher was to understand the meaning of the information as delivered by the participants and how they made sense of the lived experience. Understanding of the participants was enhanced by the use of interviews combined with document review for data analysis.

The use of interviews in qualitative analysis requires the participants to meet eligibility requirements, which make them suitable for answering the research question emphatically (Johanssen, 2016). Johanssen (2016) mentioned a well-constructed interview enables the participants to speak and induce the actual meaning of the phenomenon. Upon completing the interviews, the participants were asked if they had any public documents that could be provided, such as training information or reports. Yin (2018) expressed document review as the use of existing information on the subject-matter that provides a more detailed understanding as it expands on the data collected by other means.

Member checking was also a valuable tool in the data analysis process of this study. Member checking is a participant validation technique, whereby the data or results are returned to the participant to check for accuracy (Birt et al., 2016). When the researcher uses the member checking technique, participants are allowed to verify their perspective of the event, which brings clarity to the realities of the interpretations of the researcher (Iivari, 2018). The use of multiple techniques, such as member checking, promotes credibility. There may be situations in which a researcher lacks the requisite knowledge, but the use of member checking can enhance the experience and enable the researcher to acquire a better sense of the phenomena (Liao & Hitchcock, 2018).

Von Bertalanffy (1972) discussed the importance of scholars viewing security as an entire system. This language had a correlation with other theories such as Coole and Brooks (2014), who indicated the need for a holistic approach. The research conducted for this study garnered a holistic approach by considering all aspects from the internal employee, to hackers, to the role of IT, and the role of management. Lee and Kang (2015) developed a concept citing the use of multiple techniques would be a more effective strategy to fight cyberattacks than a single method; furthermore, I analyzed the responses of participants where the interview questions were designed to investigate emerging themes for multiple strategies.

By understanding the scope and limitations, the researcher can determine a credible and effective analytical technique. Appelbaum, Kogan, and Vasarhelyi (2017) stressed the importance of the researcher understanding the nature, distribution, and limitations of the population that is being tested. In case studies, such as this one, the purpose is to obtain a precise evaluation of the participants and the event.

Also, in this study, I used thematic analysis. Braun and Clarke (2016) explained a thematic analysis as a usual form of analysis when conducting qualitative research where there is a process of theme-discovery evidenced by the language used. Appelbaum et al. (2017) discussed that data analysis might consist of evaluating results and having the ability to integrate those results with traditional findings. Thematic analysis embroils the observation and recording of patterns in data and signifies a word or phrase that is representative of the data and captures the essence of the information collected (Clark & Vealé, 2018). The thematic analysis was a transitional process between data collection and data analysis because I was provided the ability to decode and encode.

The process involved a detailed analysis of the emerging themes by color-coding and utilizing Yin's (2018) 5-step process to compile, disassemble, reassemble, interpret, and compile. I created an Excel spreadsheet to organize and then evaluate the findings of the interviews. Trudel, Murray, Soyoung, and Shuo (2015) shared based on the consumer, coding, especially methods such as traffic light coding (TLC) can create tremendous impact by increasing the depth in which the researcher can process information. The strategies included preparing (compiling), reducing the data into themes (disassembling), organizing the data (reassembling), and representing the data in figures, tables, or discussion (interpreting and concluding).

Reaching a saturation point in the thematic analysis is essential to validity in qualitative studies, yet the process of achieving saturation is often left ambiguous, promoting the need for clarity in the process; additionally, this may include coding that justifies the sample size. The key to understanding an analytic method lies in understanding the logic behind the phenomenon and how to incorporate that information into the research process. In this study, themes were broken down to yellow (possible strategy), red (interesting point of view which may require follow-up), and green (creating a point of view). A useful framework for thematic analysis should include codes applicable to the emergent themes (Moira & Brid, 2017). In the framework created by

Moira and Brid (2017) the researchers suggested the researcher ensures familiarity with the data, develops codes applicable to the various themes, searches for and review emerging themes, then defines and composes the results.

Reliability and Validity

Reliability and validity are methods that may be undertaken in the research process to deliver findings accurately reflecting the data. Kelly, Fitzsimons, and Baker (2016) described reliability as the extent to which the research has reached a level where it is consistent, stable, and repeatable; additionally, Kelly et al. explained availability as the extent to when the research may be deemed as an accurate representation of the even and free from bias. Reliability and validity bring rigor to the study, such as truth, value, consistency, neutrality, and applicability, consequently, validity refers to the integrity and reliability refers to consistency (Noble & Smith, 2015). Multiple sources of data add value to research because of the deliverance of an in-depth account of the phenomena as viewed from the participants. Methodological triangulation may include interviews, surveys, observations, and document reviews (Morgan, Pullon, Macdonald, McKinlay, & Gray, 2017). In this study, I made use of interviews and document reviews combined with member checking.

Reliability

The level of confidence placed on the results of a study should be one of the most critical concerns of the researcher. When considering reliability (dependability), the study should be able to be reproduced and should be aligned with the objectivity and credibility of the study. Yin (2018) stated member checking could provide reliability within a qualitative design. For this study, reliability and dependability were addressed through member checking of data interpretation. The use of member checking technique places the participants in a position to function as co-interpreters to make sense of both their organizational realities and researchers' interpretations of those realities (Iivari, 2018). Member checking was an effective avenue for me to ensure the findings were presented accurately and reflected the participants' experiences and perspectives. Yin described dependability as the accountability that must be provided for the changes and resolutions that occur in the research process.

Validity

Validity or trustworthiness should be reflective of the authenticity of the results. Noble and Smith (2015) defined validity as the integrity and application the researcher administered to the study allowing the deliverance of accurate findings. The researcher can practice one-way validation by inviting the participants to comment on the final transcript or responses to ensure the information is a fair reflection of the phenomena (Noble & Smith, 2015). Four alternative criteria exist that define the trustworthiness of qualitative research: credibility, transferability, confirmability, and data saturation. By using multiple sources of evidence such as archival data and interviews, allows for comparison in the research study, which assists in data validation (Canales, 2015). I used interviews, member checking, and document review. Even though the participants were asked, I was also able to locate archival data from magazines and newspaper articles that aligned with the information gathered from the interviews.

Credibility, as defined by Twining, Heller, Nussbaum, and Tsai (2017), relates to the believability of the research findings. I used methodological triangulation, whereby multiple perspectives are viewed per the interpretation of a single set of data. The methodological triangulation process consisted of data from interviews, document review, and member checking. Member checking is a valuable method to ensure credibility. Marshall and Rossman (2016) suggested e-mail is commonly used to follow up interviews with questions for clarity or elaboration. I used e-mail for the member checking. I used e-mail to add an attachment of my analysis and summary of the interview. Participants were invited to confirm or add to my summary by responding to the e-mail. Tracy (2010) indicated that credibility is achieved by employing a full description, triangulation, crystallization, and member reflections.

Transferability, as described by Noble and Smith (2015), refers to findings that can be applied to other settings or groups; the findings from this study provided useful strategies to reduce the fiscal impact of cyberattacks to a multiplicity of organizations and industries. Additionally, Cope (2014) suggested transferability has been reached when an individual not involved in the study can relate the findings with their own experiences; furthermore, the researcher should provide detailed information regarding the participants and research context that will allow the reader to assess the findings' capability of being transferable.

Confirmability relates to the way the researcher demonstrates how the data represent the participant's responses and not the viewpoints of the actual researcher (Cope, 2014). Cope (2014) indicated the researcher should obtain confirmability by using a definitive conclusion detailing how the interpretations were reached and demonstrate the findings came directly from the collected data. I exhibited confirmability by providing quotes and emerging themes. Cope also said confirmability had been ensured when a well-trained, experienced qualitative researcher supervises an interviewer. A committee throughout the research process managed me.

Data saturation, as defined by Fusch and Ness (2015), has been reached when the researcher has exhausted the need to collect any more samples because no new data is provided in interviews, no new themes emerge from the data, and the study has enough information that it can be replicated. Denzin (2012) suggested the use of methodological triangulation could have a significant impact in enhancing the ability to achieve data saturation. Data for this study were collected through semistructured interviews and document review. The combination of data sources also helped to ensure data saturation was achieved. Malterud et al. (2015), who stated the more relevant information contained in the sample, the number of participants required to reach data saturation is lessened, introduced the concept of information power. I achieved data saturation by using semistructured interviews and document review.

Transition and Summary

Presented in Section 2 was a detailed view of the qualitative single case study involved in this research. This section consists of pertinent segments of the study, whereby, I identified my role as the researcher and the primary data collection instrument. The ethical principles of this study were upheld as I abided by the required guidelines of the 1979 NCPHSBBR’s Belmont Report. I ensured the participants were comfortable and had a clear understanding of the process per respect of person, beneficence, and justice. After obtaining Walden IRB approval, I provided and discussed with each participant the Informed Consent Form and implementation of the interview protocol. Semistructured interviews were conducted with the targeted population face-to-face and via telephone based on the availability of the participants, combined with document reviews. Reliability and validity were addressed, whereby the use of member checking and document review enhanced validity.

In Section 2, I explained how I came to view the phenomenon through the lenses of the participants in relation to the fact that the collection of data should enable this to happen as a perspective is obtained from various angles and giving way to an accurate picture of the lived experience. The participants were composed of IT administrators and management from one major U.S. airline who have implemented strategies to reduce the fiscal impact of cyberattacks. Each participant had more than 5 years of experience in their industry and was able to provide accurate details of the problem under study. Participants were assigned numerical codes to keep them confidential. I reached data saturation when there was no new information.

Also included was an explanation of the use of coding and the identification of recurring themes by use of thematic analysis, which is a widely used form of analysis in qualitative research of theme-discovery (Braun & Clarke, 2016). Appelbaum et al. (2017) believed if the researcher can understand the scope and limitations of the study, there is the ability to determine a credible and efficient analytical technique.

The approach to Section 3 in this study provides a summary of the findings while addressing such topics as themes and social change. Data were collected and placed on a spreadsheet using color-coding. The results of the data are shared in Section 3, and the emerging themes were centered on proactivity, a strong management presence, and education and training. In Section 3, the participants discussed the insider hacker, who can be easily overlooked, yet highly impactful in damaging the system. Also shared is a reflection, summary, and conclusion of the study.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative, single case study was to explore strategies IT administrators and airline managers use to reduce the fiscal impact of cyberattacks. My research included an analytical view of a conceptual framework. Data collection for this study included semistructured interviews of seven participants who had more than 5 years of experience planning or responding to a cyber event; additionally, the participants were required to have lived the experience. I used Yin's (2018) 5-step process of compiling, disassembling, reassembling, interpreting, and concluding for my data analysis.

The conceptual framework for this study was von Bertalanffy's general systems theory. According to this theory, individuals should view security as a whole system. I was able to identify several themes per my data analysis. If all the strategies expressed in these themes were implemented, they could be a highly effective means towards reducing the financial implications of by cyber events. The themes that provided meaningful strategies to reduce the fiscal impact of a cyberattack included proactive plans with education and training, strong management presence and directives, and an incident response plan. As I discuss each of these themes, I provide detailed findings inclusive of applicable theories, references, and responses of the participants.

Presentation of the Findings

The overarching research question guiding this qualitative single case study was: What strategies do IT administrators and managers in the airline industry use to reduce the fiscal impact of cyberattacks? In response to this question, I researched several theories. I conducted data analysis by using thematic analysis and coding. When using thematic analysis of qualitative data, the researcher can identify patterns or emerging themes that provide vital information regarding the issue (Moira & Brid, 2017).

I created a spreadsheet based on the interview responses and analyzed the responses in conjunction with the correlating theories and information obtained from the literature. By involving various methods as suggested by Trudel et al. (2015), I processed the information with a view toward providing valuable knowledge in the subject area. I coded the responses using the colors of yellow, red, and green. Yellow represented that a possible strategy had been identified, the red indicated an interesting point of view where follow-up may be required, and the green indicated the participant might be introducing a new point of view. Before preparing and organizing data by reducing the data into themes and representing the data in a table, I examined Moira and Brid’s (2017) framework for thematic analysis.

Table 1

Thematic Analysis - Possible Strategies Determined by Data Analysis

Participants	Strong managers	Education & training	Adherence to corp & gov policies	Preparation thru operational planning	Practice & drills	Inside threat
5	X	X		X		X
6	X	X		X		
7	X	X	X	X	X	X
8	X	X		X	X	X
9			X	X	X	
10		X	X	X		X
11	X		X	X		

Note. Table 1 denotes the correlating themes as derived from participant responses based on occurrences and lived experience with the phenomena. The responses have formulated possible strategies that organizations may use to reduce the fiscal impact of cyberattacks.

Emergent Theme 1: Proactive Plans with Education and Training

One of the themes that quickly manifested was that organizational leaders must be proactive in enacting strategies to reduce the fiscal impact of cyberattacks. The elevation of digital literacy, skills, and awareness among leaders of organizations should be of utmost priority (Cirnu, Rotuna, Vevera, & Boncea, 2018). The phenomenon of cyberattacks is becoming more sophisticated, and the number of organizations being affected continues to grow. For this reason, coordinated efforts at the organizational, regional, and global level are vital (Eugen & Petrut, 2018). Data received from the interviews and document review substantiated the importance of education and training.

The participants promoted education and training, specifically P5, P7, P8, and P11. Regarding the organization, P7 stated, “The best medicine is prevention, and you’re not going to get that from the system you create alone but also training and educating the end-user." Huang et al. (2018) cited education as the primary strategy to reduce the fiscal impact of a cyberattack because organizations should understand the importance of protecting vital company information and customers. The responses provided by P5, P7, P8, and P11 are consistent with the general systems theory by viewing cyber events holistically.

Society has a growing dependency regarding the use of AI to detect suspicious activity such as unusual patterns and to filter e-mails, thereby preventing a harmful situation (Wirth, 2018). P9 shared a document (report) that management of several major airlines plan to institute AI initiatives with customer service, allowing AI to work beside the agents and not for them. For reasons such as the growth of AI, P7 stressed, "Regular practice exercises should be implemented so when an attack occurs, individuals will be aware of and know how to handle the situation." P8 was also a strong proponent of preparation through training. Both P7 and P8 indicated daily system scan and updates are necessary and P8 shared a document that was publicly generated, announcing how one carrier plans to stay ahead of threats by implementing advanced e-mail security technology. Insight was shared by P7, who believed the ability of management to have a robust plan in place is one of the most effective strategies an organization can adopt to reduce the fiscal impact of cyberattacks.

Much attention has been directed to cyberinfrastructure and strong cybersecurity, and this attention has led to cybersecurity turning into a discipline (Patrascu, 2018). Because of the increased focus, organizations and universities alike have heightened the education and training aspect of cybersecurity. Cyberattacks have become a real threat, and the organization must understand prevention is the foundation of all strategies (Patrascu, 2018). There was a disclosure by P7 that mentioned it is the responsibility of organizations to guard and protect against the devastating financial impact of cyberattacks. “The lack of education and training can be a serious barrier for an organization attempting to combat an attack,” stated P8. Organizations are much more stable if they have well-prepared staff and a solid plan in place. Several of the participants described an educated and prepared IT and management team, practice drills, written procedures during an event, and alternative methods are essential for continued operations during an event.

P10 added, “One of the easiest and cheapest methods to prevent damage in cyber incidents is education and training.” Proper management in the case of an event is vital in reducing the fiscal impact and mitigation of reputational loss; furthermore, proper planning keeps all individuals working cohesively and invokes order in the presence of a chaotic situation (Brown, 2016). The chaos theory introduced by Burns (2016) is apt to be applicable in cases where there was no proper planning; thus, external forces promote an environment of chaos, and effective management is necessary. A small change can make the system behave entirely differently and can teach managers a lot about making wise decisions in a complex environment.

Table 2

Frequencies from Thematic Analysis for Proactive Plans with Education and Training

Emergent theme	References	Frequencies
Theme 1: Proactive plans with education and training	Education	30
	Training	27
	Organization	15
	Planning	25
	Management	18

Note. Table 2 displays the participants' references and frequencies in interviews and documents for the first theme; proactive plans with education and training.

Emergent Theme 2: Active Management and Directives

The management team is usually the first voice of the organization when a cyberattack occurs. P7 shared a document regarding corporate governance, which stated, "The board shall look to management to disseminate information and speak to the public." Cyberattacks are one of the most evolving and complex issues with which management must contend; therefore, management should provide strategies for profit maximization, loss minimization, and the safety of lives and properties (Akinwumi, Iwasokun, Alese, & Oluwadare, 2017). Five of the seven participants spoke regarding the importance of management. Management involvement, according to P5, was listed as one of the primary strategies to successfully combat a cyberattack, and P6 said, "It is necessary that the leadership is effective, as they have the responsibility of crowd control and issuing directives during a cyberattack." In the case of an event, P8 suggested management should have a strong presence and should keep the team informed. In conjunction with the participants mentioned above, P11 mentioned waiting on directives from corporate; however, much focus should remain on the employees. The point was made by P11 suggesting slow or lack of response from corporate management as a barrier for his organization when an event occurs. A manual explaining procedure provided by P11 was in alignment with the five other participants who expressed how important the role of management is during a cyberattack. The results indicated the actions of leadership, whether board or management, could harm or save an organization.

Strong leadership is a critical factor in protecting the organization’s valuable assets. Mossburg (2015) stated management should be viewed as the defender of the fiscal health of the company’s performance. Organizations display more power in the control of cyberattacks when there is an established managerial team devising strategies, preventive security measures, and communicating with IT. Furthermore, having a capable management team could save an organization $457,691 per breach (Krishan, 2018). The promotion of active management was prominent amongst the emerging themes provided by the participants and was also indicated in the document review as presented by P8. The document announced the hiring of a new chief information officer who had doubled the cybersecurity team and advised all employees to view this as a matter of resilience.

The internal attacker may be more accustomed to the environment and have a more significant financial impact than an outsider. The internal customer is tied to the organizational intranet, causing them to be prone to phishing scams, as explained by P8. Liang et al. (2016) shared that disgruntled personnel may also be responsible for purposely introducing an attack. P10 stated, “One of the things we always try to emphasize is human factors are the largest challenge and the potential to do the most damage.” The angle taken by P5 and P6 viewed the internal attack as a failure of personnel to take action, which may also be viewed as a lack of education and training provided to personnel. A document regarding the global security program of a major carrier was provided by P5. Included in the document was information that would heighten the awareness of employees and a description of what to look for in terms of phishing and the insider. The report also contained an explanation of the release of monthly test e-mails to check for employees who may engage in phishing and educating the employee; consequently, there has been a reduction in phishing per that carrier and affiliates.

P7 mentioned the importance of organizational leadership remaining in compliance with governmental regulations. Comments offered by P10 advised, “Leadership in my organization spends too much time on the interpretation of government regulations which impose numerous constraints on the ability to operate or repair the systems.” Cairney (2012) placed attention on the instability and disorder in politics and policies and unites them with complex system behaviors, per the complexity theory. Government regulations are necessary to protect computer systems and IT. Without new legislation, there is uncertainty as to how the Federal Trade Commission (FTC) will regulate security and other data practices; however, the need for Congress to introduce effective legislation continues to grow (Gordon, 2016).

Designing and agreeing on different aspects of the regulations may take a long time and often stand to become outdated. Despite this fact, leaders of organizations should no longer minimize the ability of the government to protect them as they may have done when confronted with other threats (J. Collier, 2018). Organizational leaders should apply best practices as precursors to the standards that may be employed as a basis for a similar standard (Srinivas, Das, & Kumar, 2019). P7 provided with a document on the website for a major carrier labeled *The Contract of Carriage*. The document was a statement of administrative protocol, not a contractual agreement. The material provided detailed insight into regulations, policies, and procedures.

The responses shared by the participants illustrated the important role of management in cybersecurity. The role of management in terms of cyberattacks has captured the attention of researchers. Soomro, Shah, and Ahmed (2016) shared literature that shows the development and implementation of cybersecurity policy is crucial and should include aspects such as the human factor, policy awareness, training, and the integration of technical and managerial exercises. All of the elements mentioned are essential elements of security management.

Table 3

Frequencies from Thematic Analysis for Active Management Presence and Directives

Emergent theme	References	Frequencies
Theme 2: Active management presence and directives	Management	18
	Directives	8
	Corporate	7
	Leadership	2
	Government	9
	Regulations	10
	Internal User	15

Note. Table 3 displays the participants' references and frequencies in interviews and documents for the second theme; active management presence and directives.

Emergent Theme 3: Incident Response Plans

The majority of participants described the current processes their organization has in place include an immediate shut-down of the system, and individuals revert to working manually without the use of technology. The ability to work manually is in alignment with one of the main strategies of education and training. P5 shared, "Once the internal and external customers have been secured, pencil and paper is a viable option." P5 also indicated less experienced agents might not have been trained or are not familiar with manual entries that would keep operations running without technology. Less knowledgeable individuals could pose as barriers but shutting down the system is vital.

P6 shared a document from an event that disrupted operations for 24 hours and delayed hundreds of flights for days. The document as issued from management advised that all flights were stopped for 24 hours and travelers were to be rebooked or accommodated in a hotel with no additional fees. The airline industry is an industry comprised of very complex systems, which may have been a factor Lee and Kang (2015) considered when they discussed the multilayer theory, whereby one layer can compensate for the limitations of another layer. Multilayering is a concept that is a cornerstone to aviation security.

P6 discussed redirecting the customers, if possible, to another facility or copying data to keep operations from being interrupted. To develop strategies that could reduce the fiscal impact of a cyberattack, IT administrators should have a thorough understanding of the network configuration, and they should be aware of the public application profile, such as the IP address and access applications on the IP addresses (Major, 2017). Lastly, Major (2017) suggested IT administrators should channel attacks to an alternative system to maintain operations and protect the network and infrastructure of the policy of the organization. Manual operations in the case of an event were of importance to P7, who stated, “When tasked with the use of manual operations, most participants agreed to the fact individuals displayed a willingness to participate in the necessary processes.” Modern technology has its place, but manual operations should never be dismissed, as is evident by some of the participant responses.

Based on the responses of the participants, having an incident response plan in place should be of utmost importance. The program should protect personnel, assets, information, and any entity that may cause an interruption to operations (R. Collier, 2016). Brown (2016) stated an estimated 72% of organizations have a response plan in place. Cybersecurity should become the focus of the entire organization and not isolated to IT administrators.

Table 4

Frequencies From Thematic Analysis for Incident Response Plans

Emergent theme	References	Frequencies
Theme 3: Incident response plans	Systems	17
	Shut-down	16
	Manual	7
	Network	10
	Plan/Preparation	35

Note. Table 4 displays the participants' references and frequencies in interviews and documents for the third theme; incident response plan.

An Analytic Dichotomy of Findings with the Conceptual Framework

This qualitative study was grounded to the general systems theory by von Bertalanffy, who developed this theory supporting the fact that security, based on design and operation, should be viewed as a whole system (von Bertalanffy, 1972). Von Bertalanffy (1972) advised in the event of a cyberattack, organizational leaders cannot secure only some sections of the system or the organization because then other segments are left vulnerable. The general systems theory was a good foundation for this study because cyber events, when reacted to as a whole and not in segments, increases the chances of the managers leading the organization to adaptability, thus, reducing devastation.

When the whole system has been addressed there is uniformity, and no one area gets more attention leading to an overall focus on the entire organization. Cyberattacks demand a holistic approach to reduce the fiscal impact. Consider the response of the participants in addressing the first theme, where they unanimously thought being proactive is a priority. Study data reveal proactivity includes every aspect of prevention in the entire system; furthermore, how to continue operations during the event. Von Bertalanffy (1972) suggested interrelatedness and interdependence are factors demanding awareness. The need for general systems consciousness is pertinent and requires the focus of multidimensional sites on management.

There exist other theories that are in conjunction with the implementation of the whole system. Viuker (2014), who stated several strategies that should be in place to reduce the financial implications of a cyberattack include a level of understanding for the security needed, developed one such theory. Viuker also suggested there should be a roadmap to strengthen security monitoring, and lastly, there should be clear objectives, processes, costs, timelines, and a method of assessment. Coole and Brooks (2014) introduced the security in decay system, which also addresses the need for a holistic approach; consequently, Cole and Brooks supported the theory that all elements must be maintained at optimum operating levels to be proactive. If organizational leaders were to develop a proactive, holistic approach towards the handling of cyberattacks, such events could be prevented. Additionally, the fiscal impact could be minimized, and so would information loss or system paralysis.

Supporting the thought process of reducing the fiscal impact of cyberattacks, Kim, Kim, Hong, and Oh (2017) discussed the various types of security incidents and how handling them requires security education and training. In viewing the results of education and training, there was a clear connection with the second theme regarding the importance of management. During each of the interviews, at some point, management was discussed. Perhaps this is yet another way to ponder the general systems theory (von Bertalanffy, 1972) because to reduce the fiscal impact of an event, an everyone must be engaged, from the agents to IT, management, and the board of directors. Another correlating theory would be the complexity theory (Cairney, 2012), whereby it is believed a network of elements is necessary to interact and combine to produce systematic behavior. The verbiage may have been slightly different, but nearly all participants spoke about education, training, and the need for active management.

All participants regarding immediately shutting down the system in the case of an attack shared the third theme. While this process is deemed valid by the participants and may be a necessity, Christensen et al. (2015) introduced a contrasting theory called disruptive innovation, whereby the need is emphasized for a more straightforward, scalable, system-changing solution, as the belief here is technology has become the victim of its own success. P7 spoke strongly about reverting to the use of pencil and paper to keep operations open in the event of an attack. This theory may be one requiring more attention because, although education and training were thematic, P11 linked this theme to the malicious insider (internal customer).

The internal customer or human factor presents a considerable security risk to organizations. The internal customer has access to information systems (Omar, Mohammed, & Nguyen, 2017). Sometimes the insider may have malicious intent or may accidentally cause a system problem, supporting the reason why education, training, and effective leadership are all part of the whole-system as theorized by von Bertalanffy (1972).

Placing the attention on one area of a cyber event is not an effective strategy in reducing the fiscal impact of a cyberattack. As I reflect on this segment of the study and the theory of von Bertalanffy (1972), all sectors must be secured and interrelatedness and interdependence demand awareness. Viuker (2014) discussed the need for a roadmap to strengthen security monitoring, and Kim et al. (2017) stressed the requirement for education and training to minimize cyberattacks. Lastly, Cairney (2012) shared the fact that a network of elements is necessary to produce systematic behavior. As various theories were combined for consideration, I found support for the general systems theory of viewing the entire system, inclusive of the organization, when considering being proactive in cyber phenomena and thus, reducing the fiscal impact.

Application to Professional Practice

In this qualitative single case study, I presented findings that are conducive to the professional practice of organizations for various reasons. First, there is a revelation that organization leaders must develop a profound understanding of the impact a cyberattack can have on the organization fiscally; thus, creating a motivation to create proactive measures. Secondly, management, inclusive of the IT administrators, is crucial. In the case of an event, decision-making, policies and guidelines, directives, operations, and a constant presence, all are of importance. Lastly, the findings proved a strong desideratum for education and training.

People, Planning, and Preparedness

Unfortunately, there are organization leaders who are of the belief that the vigorous defenses they have in place are enough to protect them from an attack; thus, they fail to be proactive. However, cyberattacks have the propensity to aggregate the global economy by approximately $445 billion per year, which should cause leaders of organizations to consider taking a more proactive approach to cyberattacks (Samtani et al., 2017). The participants perceived the ability to *get ahead of the problem* could reduce or prevent the devastation of a cyber event. Being proactive could be in the form of education and training exercises such as drills, frequent checks, and focus on the human factor (internal customer).

The insider places a significant role in organizational misconduct. Human factors are responsible for 95% of all security incidences, and it is this factor that is the weakest link of security (Gyunka & Christiana, 2017). Gyunka and Christiana (2017) contributed this statistic to ignorance of basic security practices, carelessness, and even disgruntled employees seeking to sabotage the organization purposely. Being proactive by focusing on the human factor is very much in alignment with education and training yet differs because the internal customer can be educated and still inflict sabotage. Liang et al.

(2016) supported the belief the human factor has a far more negative implication than outsiders do. It is beliefs such as this that highlight the importance of focusing on the insider, frequent checks, and briefings to be proactive.

One of the emerging themes included the robust use of attack drills will enable the organization to move in a mode of autopilot when an event occurs because the organization will have developed a capacity for muscle memory. The implementation of placing a focus on personnel and having a security plan, such as frequent system checks with regular drills, can make way for less exposure and an increase in system safety; furthermore, attacks will be responded to sooner allowing response procedures to be effective. Leaders of organizations should conduct regular scans to detect vulnerabilities. It is pertinent for IT administrators and management to view this as an excellent strategy of defense.

As the emerging themes from this study are considered, individuals should be able to get a clear picture of the general systems theory introduced by von Bertalanffy (1972) and the concept of utilizing the whole system. Leaders of organizations cannot use only one of these themes and expect significant results, and they must use each of them. Cirnu et al. (2018) shared that digital literacy skills among individuals and organizations are on the rise and getting more sophisticated. Christensen et al. (2015) introduced the disruptive theory stating technology is the victim of its success. This rationale supports Huang et al. (2018) reason for listing education and training as a primary strategy and a necessity.

Management is the voice that the speaks to the public. Akinwumi et al. (2017) advised that it is managerial responsibility to protect employees and consumers while minimizing loss. The chaos theory was developed by Burns (2016), who based this theory on management decisions during a crisis. The belief is that external forces present a profound influence on important decisions; thus, the decisions made by management during a time of chaos will be disruptive or effective. Each of the emerging themes had value and relate to a personal discussion with a former CEO for whom I was employed, he asked, “What part of the watch can you leave out and it still works (personal communication, Gordon Bethune, CEO United Airlines, 1995).

Effective Management

The findings in this study unanimously indicated that effective management is also a priority. The influence of management could have a profound effect on successfully reducing the fiscal impact of a cyberattack by contributing to positive cash flow through providing directives, keeping operations in performance during the event, and providing managerial support. The development and implementation of information security policy, awareness, compliance training, development of enterprise information architecture, IT infrastructure management, business and IT alignment, and human resources management are all entities that could produce substantial outcome on the quality of management and the handling of cyberattacks (Soomro et al., 2016). These factors have added great importance to the role of management; furthermore, in alignment to von Bertalanffy (1972), Soomro et al. (2016) suggested a more holistic approach to information security is needed. P6 discussed how, in the case of an event, management infiltrates the work area and immediately takes control of the situation by maintaining a calm environment and ensuring manual operations are normalized. P8 found the way management keeps the agents informed to be critical, while P7, P9, and P10 spoke on the effectiveness of being prepared, primarily through education and training offered by management to be of great value.

Van der Vegt, Essens, Wahlstrom, and George (2015) illustrated the importance of dynamic management by discussing a New Zealand earthquake where the businesses who had pre-existing organizational collaboration networks established had a better recovery than those businesses that did not. At the height of crisis levels, 29% of global aviation and 1.2 million passengers per day were affected (van der Vegt et al., 2015), which further substantiates the importance of trenchant management. In compiling the responses from the participants, emerging themes suggested in a crisis, their management displays a strong presence, provides directives and assistance, keeps the agents informed, is a resource regarding governmental policies and procedures, and projects a well-trained skillset to handle the event, thus, continuing feasible operations. One of the participants labeled governmental laws as a barrier, but many of the suggested themes are of value but would be of even more importance if supported by regulations. The participants also stated successful survival of the event is accessed by how quickly the organization can get back online, and this is achieved through effective management, the voice of the organization during a crisis.

Simplification of a Complex Environment

Individuals should possess a deep understanding of protecting the whole system. The role of active management is important, and so is the role of highly competent IT administrators. There are complexities in the position of IT that many individuals who are not technologically savvy are oblivious to. Cairney (2012) introduced the complexity theory and building on that theory was Basile et al. (2018), who described it as reducing the complexity of the volume of information flowing through the system. Organization leaders depend on the advice of IT administrators and for the creation and interpretation of policies and tools. Management should have a continuous engagement in professional development, and IT administrators should continuously engage in research, published findings, development, and participation of defense exercises, and continuously increasing knowledge of computer, networks, and policies. IT administrators should provide organizations simplification of a complex environment, thus, reducing the devastation caused by a cyberattack.

The devastation caused by a cyber event could include legal costs, increased cost/debt, higher insurance premiums, and negative outcomes for customer retention, loss of sales, and revenue. The combination of effective management and competent IT administrators can reverse or prevent these issues, which is why leaders must fathom the fiscal impact a cyberattack can inflict upon an organization. Although there is continuous growth in the IT field, there is a shortage of personnel, and the gap is widening (Mithas et al., 2018). Management should make it a critical mission to invest in IT personnel because these professionals can detect behavior patterns of hackers, create safeguards, create best practices for careless employees, and introduce new computer systems.

In some form or the other, each of the themes mentioned in the application to professional practice has been linked back to education, whether it is the agents, management, or the IT administrators. Many people consider strategies to reduce the fiscal impact of cyberattacks to be a matter that only concerns IT administrators and management; even though their role is vital, this phenomenon is one that should be managed across the entire organization (Chapman, Chinnaswamy, & Garcia-Perez, 2018). Conducting this research enabled me to conclude that through education, specific strategies are created to raise the awareness in society, so individuals may develop knowledge to protect themselves. This applies even if that technology includes social media, smartphones, Fitbit, and other technological items that have infiltrated society. Mangal (2013) introduced social media theory collaboration and integration to minimize threats. As society becomes more sophisticated, so does the need for education and training.

Implications for Social Change

As I explored strategies to reduce the fiscal impact of cyberattacks, I desired that this study depict the need for everyone to have an understanding and a plan for the cyber phenomenon. Additionally, my desire was for organizations to develop a safe and secure environment for society whether it is travel or otherwise. Perhaps if individuals were to embrace an increased understanding and the ability for timely identification of security events, it would be a great asset to social change. Samtani et al. (2017) indicated cyberattacks might affect the global economy by $445 billion per year and this is a situation that should alarm people, prompting them to seek a more proactive approach to the phenomenon. Mailloux and Grimaila (2018) related to the general systems theory (von Bertalanffy, 1972) when they stated the professionals of cyber resiliency deliver holistic solutions to maintain functionality during operations regardless of the adverse events. The increased dependence on technology has caused cyberattacks to become a real threat, and prevention is the foundation of all strategies (Patrascu, 2018). Individuals in all walks of life are now faced with an obligation during a cyber event to turn what was thought to be a weakness into a strength.

Also, when considering the implication for social change, as a result of this study, I hope there is a new focus on the influence of human factors, whereby there could be enlightenment by society to embrace an environment inclusive of education and training. Human factors may include accidental or purposeful actions by individuals who can compromise a system. The human factor is practicing sabotage and can be categorized as lazy users, economically rational users, and social users (Gcaza, Rossouw, Grobler, & Jansen, 2017). Social change could consist of a new cyber-culture to combat the situation. Cirnu et al. (2018) shared the fact that digital literacy, skills, and awareness should be of utmost priority. Many individuals perceive security measures as a waste of time and ignore them. The view shared by Patrascu (2019) revealed a culture involving cybersecurity involves safe practices and an awareness of cyber threats. Eugen and Petrut (2018) advised everyone is vital as a coordinated effort is required at all levels of society, including globally, to deliver an education of the cyber phenomenon. One of the participants of this study shared the observation indicating the best medicine is prevention, which will not come from the system but in the education and training of the end-user.

This study could promote a shift in the mindset of all individuals to place more focus on the importance of cybersecurity. A social change could include people who add to their attention an understanding of cyber-health. Akinwumi et al. (2017) disclosed cyberattacks are a very complex issue, and the primary reason individuals should consider the implementation of strategies beneficial to the safety of lives and properties. Lastly, social implications may include legislators who are willing to introduce new regulations that will allow the consumer to have the comfort of knowing their personal information is protected.

Although further research is needed, the findings of this study produced themes that could be conducive to reducing the fiscal impact of cyberattacks. I believe the implications for social change discussed in this section are vital for the future. If society embraces a plan and a reliable process, the financial devastation of a cyber event could be drastically reduced. The plan, combined with education and training, elevates preparation and further reduces negative economic implications. Technology is steadily increasing, and with that understanding, so should the strategies to reduce the fiscal impact.

Recommendations for Action

This qualitative single case study was conducted to explore strategies to reduce the fiscal impact of cyberattacks. Research of such exposed a lack of national legislation. No new legislation regarding cybersecurity has been introduced since about 2008;

however, additional measures are needed and would cost more than $150 million per year, but no new funds are authorized (Srinivas et al., 2019). Some laws in place are vague, and some lack sufficient privacy protections. There are antiquated and insufficient laws in place; therefore, I recommend a call for action from the government to introduce new and improved legislation. Srinivas et al. (2019) suggested a new set of cyber standards and laws are needed to help the government with an expectation for departments to adhere and exceed. The challenge of cyber events is steadily on the rise, and organizations are vulnerable. I also recommend this legislation include protections against human factors. Insider threats are not new but emerging and as damaging as external threats; furthermore, the insider threats have been overlooked for years with no clear standards to protect systems from these threats (Mills, Stuban, & Dever, 2017). Gisladottir, Ganin, Keisler, Kepner, and Linkov (2017) expressed the belief numerous scientists are focusing on cybersecurity when there should be more psychologists, economists, and people who specialize in dealing with the human factor.

Resilience may be defined as the ability displayed by an organization to absorb, recover, and adapt in the event of an attack (Gisladottir et al., 2017). Participants shared several barriers that prevented them from being resilient, which included a lack of training, such as new agents who are not familiar with manual processes, delays because of interpretation of laws, and a lack of communication from management. I recommend a call for action, whereby all organizations promote a culture of awareness and education regarding cybersecurity with a heightened sense of resilience as a strategy. By being proactive and by planning and preparation, organizations can overcome the previously mentioned barriers. Concerning innovation in technology, the airline industry guides the way and has experienced significant growth as a result (Lykou, Anagnostopoulou, & Gritzalis, 2019). With growth come challenges, such as smart devices; thus, resiliency is vital in the maintenance of dynamic growth, safety, and security. Also, with the new, smart technologies, comes a vast attack surface and severe impact on organizations. The aftermath of an event may cause loss of reputation and clients' trust, stopped production, and loss of intellectual property, and may have a tremendous fiscal impact in general (Carías, Labaka, Sarriegi, & Hernantes, 2019). Leaders of organizations must develop a new cyber-culture of being proactive and resilient.

Dissemination of this study will include submissions to journals, conferences, seminars, and the classroom for students in higher education. In conjunction with responding to a call for papers, I will also seek publication via databases such as ProQuest and EBSCOhost. I am fortunate to have an available platform as a public speaker that has enabled me to share vital information about various topics. Strategies that airline managers and IT administrators can implement to reduce the fiscal impact of cyberattacks will be a topic that takes center stage.

Recommendations for Further Research

It is pertinent that the future is intelligent. I make this statement because of the emergence of AI, and despite society's hesitance, there is an eagerness to embrace AI (Wirth, 2018). The definition of AI, as provided by Wirth (2018) is intelligence by using machines or an intelligent agent; basically, it is computers that have the intellectual capacity to replace humans in a specific activity. A report conducted through the

McKinsey Global Institute shared the finding that 30% of the hours worked globally could be automated by 2030, depending on the speed of adoption (Manyika, Lund, Chui, & Bughin, 2017). Considering we are living in the age of Siri and Alexa and the vigorous growth of AI, there are more data to be aware of that could cause challenges.

My recommendation for the future is increased research on AI with an emphasis on security. Even though AI is experiencing exponential growth and making life more comfortable, it is also introducing new opportunities for cyber events (Lykou et al., 2019). AI has had a significant influence on organizations as well as the average household, which has caused society to become even more vulnerable to cybercrimes.

The limitations of the study regarding AI were contributed to the fact that this technology is still in its infancy. As research is being focused on the limitations of AI, scholars would be remiss to discard the theory of disruptive innovation (Christensen et al., 2015). Christensen et al. (2015) as discussed in the conceptual framework and suggest that technology has become the victim of self-inflicted success. Albeit that academic literature and articles have been published regarding the phenomena, only a limited amount of research is available in this area to accurately assess the risks and trends (Romanosky, 2016). This qualitative single-case study design may have limited the insights gathered for this study, and therefore, further research utilizing other designs is imperative concerning all topics about cyberattacks.

Reflections

I remember my father telling me, “It’s not about the destination, but the journey” (personal communications, Clarence Monix, 1980). This doctoral program has been a journey that will forever be embedded in my heart and brain. When I was tasked with the job of developing a topic for my business study, I changed topics several times until I arrived at strategies to reduce the fiscal impact of cyberattacks. In all honesty, this topic is one I have never given serious thought. Ironically, I saw the error of my ways as I researched various aspects of the existing scholarship, such as when I considered the human factor. The more I researched, the more excited I found myself about this topic, so much so, that I plan to continue research in this area and even conduct a few seminars, as I periodically undertake speaking engagements.

This journey introduced me to implementing theories, synthesizing scholarly materials, critical-thinking, various types of research methods and designs, and a heightened knowledge of academic writing. I have now developed a keen sense and interest in this subject matter. Before this journey, my personal bias was that organizational leadership already had an in-depth knowledge not only of the phenomenon but had processes in place; hence, it astounded me to realize how false that belief is. Rivers, Rees, Calanchini, and Sherman (2017) explained that for personal bias to be present, an individual must have believed a particular thing over an extended period and to the point it can spread within that person’s social circle. Even if I did not bring a change in even one participant, they bought about a change in me. I came to realize that the knowledge concerning expectations held by specific individuals or circles and their willingness to accept what is authentic may require face-to-face encounters. Now I know what questions to ask of organizations and what advice and support to offer. Most of the participants, whether interviewed face-to-face or via telephone, felt honored to participate in this scholarly research and the ability to contribute to a heightened awareness of cyber events.

Conclusion

It has been shared that cyber-threats may be one of the gravest national dangers to the United States. The continually growing threat has an estimated total cost of events at approximately $8.5 billion annually (Romanosky, 2016). This statistic supports the fact that there is a need for strategies to reduce the fiscal impact of cyberattacks. This study uncovered valuable strategies. Revealed was the need to be resilient, that organization leaders must create a culture including strong managerial and IT leadership, education, and training, combined with an incident response plan.

There is an urgent need for new legislation and competent leadership to enforce these new laws. There is a dire need to focus on the human factor and that this entity is managed accordingly. The Internet is so crucial in our daily lives, and dependence upon it has a vast amount of growth on an annual basis. A study conducted by Bakdash et al. (2018) illustrated cyberattacks might endanger us in more ways than economically, but also physically and politically; moreover, results of this study are in alignment with Bakdash et al., indicating that enhanced awareness of the phenomenon may improve through the optimization of human and technical capabilities. No longer should the question be if an attack will occur, but when, which strengthens the need to embrace people, planning, and processes.

References

Ablon, L., & Libicki, M. (2015). Hackers' bazaar: The markets for cybercrime tools and stolen data. *Defense Counsel Journal, 82,* 143-152. doi:10.12690/0161-8202-82.2.143

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility, 4*, 65-88. doi:10.13052/jcsm2245-1439.414

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., & Oluwadare, S. A. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology, 36*, 1271-1285. doi:10.4314/njt.v36i4.38

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

Antonino, P. D. (2015). The instrumental value of conceptual frameworks in educational technology research. *Educational Technology Research Development, 63*, 53-71. doi:10.1007/s11423-014-9363-4

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). An introduction to data analysis for auditors and accountants. *CPA Journal, 87*(2), 32-37. Retrieved from http://www.cpajournal.com/

Ashby, W. R. (1991). General systems theory as a new discipline. *Facets of Systems Science, 7*, 249-257. doi:10.1007/978-1-4899-0718-9_16

Backman, S. (2015). Organizing national cybersecurity centres. *Information & Security, 32*(1), 1-18. doi:10.11610/isij.3206

Bakdash, J., Hutchinson, S., Zaroukian, E., Marusich, L., Thirumuruganathan, S., Sample, C., ... Das, G. (2018). Malware in the future? Forecasting of analyst detection of cyber events. *Journal of Cybersecurity, 4*(1), 1-10. doi:10.1093/cybsec/tyy007

Bansal, P., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal, 61,* 1189-1195. doi:10.5465/amj.2018.4004

Baral, G. (2016). Research and ethics. *Journal of Nepal Health Research Council, 14*(32), 1-1. Retrieved from http://jnhrc.com.np/index.php/jnhrc

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

Basile, G., Kaufmann, H. R., & Savastano, M. (2018). Revisiting complexity theory to achieve strategic intelligence. *International Journal of Foresight and Innovation Policy, 13,* 57-70. doi:10.1504/IJFIP.2018.095858

Belli, L., & Venturini, J. (2016). Private ordering and the rise of terms of service as cyber regulation. *Internet Policy Review, 5,* 6-17. doi:10.14763/2016.4.441

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48,* 51-61. doi:10.1016/j.chb.2015.01.039

Beverland, M. B., Gemser, G., & Karpen, I. O. (2017). Design, consumption and marketing: Outcomes, process, philosophy and future directions. *Journal of Marketing Management, 33,* 59-172. doi:10.1080/0267257X.2017.1283908

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 16,* 1802-1811. doi:10.1177/1049732316654870

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

Brantly, A. F. (2016). Aesop's wolves: the deceptive appearance of espionage and attacks in cyberspace. *Intelligence & National Security, 31,* 674-685. doi:10.1080/02684527.2015.1077620

Braun, V., & Clarke, V. (2016). (Mis) conceptualising themes, thematic analysis, and other problems with Fugard and Potts' (2015) sample-size tool for thematic analysis. *International Journal of Social Research Methodology, 19,* 739-743. doi:10.1080/13645579.2016.1195588

Braunberg, A., Walder, B., & Spanbauer, M. (2014). Ensuring and insuring global cyber resiliency. *Security: Solutions for Enterprise Security Leaders, 51,* 34-35. Retrieved from https://www.nsslabs.com/

Bressler, M. S., & Bressler, L. (2015). Protecting your company's intellectual property assets from cyberespionage. *Journal of Legal, Ethical and Regulatory Issues, 18,* 21-34. Retrieved from https://www.researchgate.net/publication/281034771_Protecting_your_company%27s_intellectual_property_assets_from_cyber-espionage

Brown, H. S. (2016). After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning, 9,* 317-328. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/27318286

Burns, J. S. (2016). Chaos theory and leadership studies: Exploring uncharted seas. *Journal of Leadership & Organizational Studies, 9,* 42-56. doi:10.1177/107179190200900204

Cairney, P. (2012). Complexity theory in political science and public policy. *Political Studies Review, 10,* 346-358. doi:10.1111/j.1478-9302.2012. 00270.x

Canales, J. I. (2015). Sources of selection in strategy making. *Journal of Management Studies, 52*(1), 1-31. doi:10.1111/joms.12101

Carcone, D., Tokarz, V. L., & Ruocco, A. C. (2015). A systematic review on the reliability and validity of semistructured diagnostic interviews for borderline personality disorder. *Canadian Psychology, 56*, 208-226. doi:10.1037/cap0000026

Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a cyber resilience investment strategy in an industrial IOT context. *Sensors, 19*(1), 1-16. doi:10.3390/s19010138

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report, 21,* 811-831. Retrieved from https://nsuworks.nova.edu/tqr/vol21/iss5/2

Center for Strategic and International Studies. (2014, June). Net losses estimating the global cost of cybercrime: Economic impact of cybercrime II. *The McAfee-CSIS Report*. Retrieved from https://www.csis.org/events/2014-mcafee-report-global-cost-cybercrime

Centre for the Protection of National Infrastructure. (2013). *CPNI Data Collection Study*. Retrieved from http://www.cpni.gov.uk/advice/personnel-security1/insider-threats

Chapman, J., Chinnaswamy, A., & Garcia-Perez, A. (2018, March). The severity of cyberattacks on education and research institutions: A function of their security posture. ICCWS 2018 13th International Conference on Cyber Warfare and Security, National Defense University, Washington, DC. Retrieved from https://books.google.com/books?hl=en&lr=&id=eHpTDwAAQBAJ&oi=fnd&pg=PA111&dq=cyber-attacks+education&ots=9TMXbd0rv-&sig=0IYKuJpsUZqMn59pVlqcNcVMNYg#v=onepage&q=cyber-attacks%20education&f=false

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

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2015). Managing ethical challenges to mental health research in post conflict settings. *Developing World Bioethics, 16*, 15-28. doi:10.1111/dewb.12076

Christensen, C., Baumann, H., & Sadtler, T. (2006). Disruptive innovation for social change. *Harvard Business Review, 84,* 94-101. Retrieved from https://hbr.org/

Christensen, C., Raynor, M., & McDonald, R. (2015). The big idea, what is disruptive technology. *Harvard Business Review, 93* 44-53. Retrieved from https://hbr.org/

Christianson, M. K. (2019). More and less effective updating: The role of trajectory management in making sense again. *Administrative Science Quarterly, 64,* 45-86. doi:10.1177/0001839217750856

Cirnu, C. E., Rotuna, C. I., Vevera, A. V., & Boncea, R. (2018). Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. *Studies in Informatics and Control, 27,* 359-368. doi:10.24846/v27i3y201811/

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology, 89,* 482-485. Retrieved from http://www.radiologictechnology.org/content/89/5/482CT.extract

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance, 6,* 13-21. doi:10.17645/pag.v6i2.1324

Collier, R. (2016). The Obama administration and incident response: A report. *Information & Security, 34,* 105-120. doi:10.11610/isij.3408

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

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum.* 41, 89-91. doi:10:.1188/14.ONF.89-91

Crespo, R. (2018) Currency warfare and cyber warfare: The emerging currency battlefield of the 21st century, *Comparative Strategy, 37*, 235-250, doi:10.1080/01495933.2018.1486090

Dan-Suteu, S. A. (2018). Boosting cyber security innovation and culture through public-private research projects. *ELearning & Software for Education, 4,* 20-25. doi:10.12753/2066-026X-18-217

Dasgupta, M. (2015). Exploring the relevance of case study research. *Vision, 19,* 147-160. doi:10.1177/0972262915575661

Denning, P. J., & Denning, D. E. (2010). The profession of IT discussing cyberattack. *Communications of the ACM, 53*, 29-31. doi:10.1145/1810891.1810904

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

Drack, M., & Pouvreau, D. (2015). On the history of Ludwig von Bertalanffy's general systemology, and on its relationship to cybernetics – part III: Convergences and divergences. *International Journal of General Systems, 44*, 523-571. doi:10.1080/03081079.2014.1000642

Ellis, R., & Marco, T. (2017, January 22). United Airlines resumes flights after temporary ground order. *CNN*. Retrieved from http://www.cnn.com/2017/01/22/travel/united-grounds-domestic-flights-because-of-it-issue/index.html

Eugen, P., & Petrut, D. (2018). Exploring the new era of cybersecurity governance. *Ovidius University Annals, Series Economic Sciences, 18,* 358-363. Retrieved from http://stec.univ-ovidius.ro/html/anale/ENG/

Fallan, K., & Lees-Maffei, G. (2016). Real imagined communities: National narratives and the globalization of design history. *Design Issues, 32,* 5-18. doi:10.1162/DESI_a_00360

Federal Bureau of Investigation, Internet Crime Complaint Center. (2017). *2016 Internet crime report.* Retrieved from https://www.ic3.gov/media/annualreports.aspx

Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning, 9,* 185-195. Retrieved from https://www.henrystewartpublications.com/jbcep

Fox, S. J. (2016). Flying challenges for the future: Aviation preparedness in the face of cyber-terrorism. *Journal of Transportation Security, 9,* 191-218. doi:10.1007/s12198-016-0174-1

Francis, K. A., & Ginsberg, W. (2016). *The federal cybersecurity workforce: Background and Congressional oversight issues for the Departments of Defense and Homeland Security* (CRS Report R44338). Washington, DC: Congressional Research Service.

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

Gcaza, N., Rossouw, V. S., Grobler, M. M., & Jansen, J. V. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information and Computer Security, 25,* 259-278. doi:10.1108/ICS-12-2015-0046

George, G. (2016). Management research in AMJ: Celebrating impact while striving for more. *Academy of Management Journal, 59,* 1869-1877. doi:10.5465/amj.2016.4006

Gillen, D., & Morrison, W. G. (2015). Aviation security: Costing, pricing, finance, and performance. *Journal of Air Transport Management, 48,* 26-33. doi:10.1016/j.jairtraman.2015.06.009

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over- and under-regulation. *Risk Analysis: An Official Publication of the Society for Risk Analysis, 37,* 1644-1651. doi:10.1111/risa.12729

Gordon, J. (2016). The need for data security legislation and cyber-insurance in light of increasing FTC enforcement actions. *Brooklyn Journal of Corporate, Financial & Commercial Law, 11,* 183-208. Retrieved from https://brooklynworks.brooklaw.edu/bjcfcl/vol11/iss1/7/

Greene, J., Gupta, R., L’Helias, S., & McCracken, B. (2017). The role of corporate boards: A roundtable discussion of where we’re going and where we’ve been. *Journal of Applied Corporate Finance, 29,* 22-35. doi:10.1111/jacf.12218

Grosz, B. J., & Stone, P. (2018). A century-long commitment to assessing artificial intelligence and its impact on society. *Communications of the ACM, 61*, 68-73. doi:10.1145/3198470

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:10.1080/07421222.2018.1451962

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of human factors in cyber security: A case study of anonymous attack on HBGary. *Computing and Information Systems, 21*, 10-18. Retrieved from http://cis.uws.ac.uk/research/journal/index.html.

Hall, M. (2016). Feature: Why people are key to cyber-security. *Network Security, 2016*, 9-10. doi:10.1016/S1353-4858(16)30057-5

Hammad, W., & Hallinger, P. (2017). A systematic review of conceptual models and methods used in research on education leadership and management in Arab societies. *School Leadership & Management, 37*, 434-456. doi:10.1080/13632434.2017.1366441

Henderson, H. (2018). Difficult questions of difficult questions: the role of the researcher and transcription styles. *International Journal of Qualitative Studies in Education, 31*, 143-157, doi:10.1080/09518398.2017.1379615

Hewes, J. A. (2016). Threat and challenges of cybercrime and the response. *SAM Advanced Management Journal, 81*, 4-10. Retrieved from http://go.galegroup.com/ps/

Hochbein, C., & Smeaton, K. (2018). An exploratory analysis of the prevalence of quantitative research methodologies in journal articles. *International Journal of Education Policy & Leadership, 13*(11), 1-17. doi:10.22230/ijepl.2018v13n11a765

Holt, T. B., Moallemi, M., Weiland, L., Earnhardt, M., & McMullen, S. (2016). *Aircraft cyber security and information exchange safety analysis for the department of commerce.* Retrieved from the Embry-Riddle Aeronautical University Scholarly Commons website: https://commons.erau.edu/publication/311/

Horowitz, M. (2012). *The diffusion of military power: Causes and consequences for international politics.* Philadelphia, PA: Princeton University Press.

Howes, L. (2015). Developing the methodology for an applied, interdisciplinary research project: Documenting the journey toward philosophical clarity. *Journal of Mixed Methods Research, 11,* 450-468. doi:10.1177/1558689815622018

Hsu, C. C., Tsaih, R. H., & Yen, D. C. (2018). The evolving role of IT departments in digital transformation. *Sustainability, 10*(10), 1-18. doi:10.3390/su10103706

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyberattack business: A survey. *ACM Computing Surveys, 51*(4), 1-36. doi:10.1145/3199674

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People, 31,* 111-133. doi:10.1108/ITP-2016-0168

Jackson, B. A., & LaTourrette, T. (2015). Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries. *Journal of Air Transport Management, 48,* 26-33. doi:10.1016/j.jairtraman.2015.06.009

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34,* 597-626. doi:10.1080/07421222.2017.1334499

Johanssen, J. (2016). Did we fail? (Counter-) Transference in a qualitative media research interview. *Interactions: Studies in Communication & Culture, 7,* 99-111. doi:10.1386/iscc.7.1.99_1

Jordan, P., Bardill, A., Herd, K., & Grimaldi, S. (2017) Design for subjective wellbeing: Towards a design framework for constructing narrative, *Design Journal, 20,* 4292-4306. doi:10.1080/14606925.2017.1352926

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management, 34,* 1043-1056. doi:10.1016/j.ijproman.2016.05.005

Kaplan, F. (2016). *Dark territory: The secret history of cyber war*. New York, NY: Simon & Schuster.

Kelly, P., Fitzsimons, C., & Baker, G. (2016). Should we reframe how we think about physical activity and sedentary behavior measures? Validity and reliability reconsidered. *International Journal of Behavioral Nutrition and Physical Activity, 13*(32), 1-10, doi:10.1186/s12966-016-0351-4

Khan, S. R. (2019). Implication of cyber warfare on the financial sector: An exploratory study. *International Journal of Cyber-Security and Digital Forensics, 7,* 31-37. doi:10.17781/P002319.

Kigerl, A. (2018). Profiling Cybercriminals. *Social Science Computer Review, 36,* 591-609. doi:10.1177/0894439317730296

Killawi, A., Khidir, A., Elnashar, M., Abdelrahim, H., Hammoud, M., Elliott, H., & Fetters, M. D. (2014). Procedures of recruiting, obtaining informed consent, and compensating research participants in Qatar: Findings from a qualitative investigation. *BMC Medical Ethics, 15,* 9-9. doi:10.1186/1472-6939-15-9

Kim, B. H., Kim, K. C., Hong, S. E., & Oh, S. Y. (2017). Development of cyber information security education and training system. *Multimedia Tools and Applications, 76,* 6051-6064. doi:10.1007/s11042-016-3495-y

Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution, 63,* 317-347. doi:10.1177/0022002717737138

Krishan, R. (2018). Corporate solutions to minimize expenses from cyber security attacks in the United States. *Journal of Internet Law, 21,* 16-19. Retrieved from http://www.journalofinternetlaw.com/

Kshetri, N. (2018). The economics of cyber insurance. *IT Professional, 20,* 9-14. doi:10.1109/MITP.2018.2874210

Lauer, C., Brumberger, E., & Beveridge, A. (2018). Hand collecting and coding versus data-driven methods in technical and professional communication research. *IEEE*

Transactions on Professional Communication, Professional Communication, 4, 389-408. doi:10.1109/TPC.2018.2870632

Lee, S. K., & Kang, T. (2015). Adaptive multi-layer security approach for cyber defense. *Journal of Internet Computing and Services, 16*(5), 1-9. doi:10.7472/jksii.2015.16.5.01

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

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems, 33,* 361-392. doi:10.1080/07421222.2016.1205925

Liao, H., & Hitchcock, J. (2018). Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation and Program Planning, 68,* 157-165. doi:10.1016/j.evalprogplan.2018.03.005

Lichterman, P. (2017). Interpretive reflexivity in ethnography. *Ethnography,18,* 35-45. doi:10.1177/1466138115592418

Lin, Y., & Chen, Y. (2018). Do less active participants make active participants more active? An examination of Chinese Wikipedia. *Decision Support Systems, 114,* 103-113. doi:10.1016/j.dss.2018.08.002

Lino, A., Rocha, Á., Macedo, L., & Sizo, A. (2019). Application of clustering-based decision tree approach in SQL query error database. *Future Generation Computer Systems, 93,* 392-406. doi:10.1016/j.future.2018.10.038

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods, 30,* 191-207. doi:10.1177/1525822X17749386

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors, 19,* 19-19, doi:10.3390/s19010019

Macak, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. *Leiden Journal of International Law, 30,* 877-899. doi:10.1017/S0922156517000358

Mailloux, L. O., & Grimaila, M. (2018). Advancing cybersecurity: The growing need for a cyber-resiliency workforce. *IT Professional, 20,* 23-30. doi:10.1109/MITP.2018.032501745

Major, T. (2017). Weaponising threat intelligence data. *Network Security, 2017,* 11-13. doi:10.1016/S1353-4858(17)30082-X

Malterud, K., Siersma, V. D., & Guassora, A. D. (2015). Sample size in qualitative interviews strategies: Guided by information Power. *Qualitative Health Research, 26,* 1753-1760. doi:10.1177/1049732315617444

Mangal, V. (2013). Systems theory and social networking: Investigation of systems theory principles in web 2.0 social network systems. *International Journal of Business and Commerce, 3,* 117-135. Retrieved from https://www.ijbcnet.com

Manyika, S., Lund, S., Chui, M., & Bughin, J. (2017). Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages. U.S. Bureau of Labor

Statistics; McKinsey Global Institute Analysis. Retrieved from https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

Maochao, X., Schweitzer, K. M., Bateman, R. M., & Shouhuai, X. (2018). Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security, Information Forensics and Security, 11,* 2856-2871. doi:10.1109/TIFS.2018.2834227

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

Mayer, I. (2015). Qualitative research with a focus on qualitative data analysis. *International Journal of Sales, Retailing & Marketing*, *4,* 53-67. Retrieved from http://ijsrm.com/IJSRM/Home.html

Mayoh, J., & Onwuegbuzie, A. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research*, *9,* 91-107. doi:10.1177/1558689813505358

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

McGraw, G. (2013). Cyber War is inevitable unless we build security in. *Journal of Strategic Studies, 36,* 109-119. doi:10.1080/01402390.2012.742013

Melnik, T. (2015). New U.S. sanctions program seeks to give government an extra tool to fight cyberattacks. *Journal of Health Care Compliance, 17*(3), 53-56. Retrieved from http://melniklegal.com/av/

Menikoff, J., Kaneshiro, J., & Pritchard, I. (2017). The common rule, updated. *New England Journal of Medicine, 376*, 613-615. doi:10.1056/NEJMp1700736

Mills, J. U., Stuban, S. M. F., & Dever, J. (2017). Predict insider threats using human behaviors. *IEEE Engineering Management Review, 45*, 39-48. doi:10.1109/EMR.2017.2667218

Mithas, S., Kude, T., & Whitaker, J. (2018). Artificial intelligence and IT professionals. *IT Professional, 20*, 6-13. doi:10.1109/MITP.2018.053891331

Moira, M., & Brid, D. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Teaching & Learning in Higher Education, 8*(335), 1-14. Retrieved from http://ojs.aishe.org/index.php/aishe-j/article/view/335

Morgan, S. J., Pullon, S. R. H., Macdonald, L. M., McKinlay, E. M., & Gray, B. V. (2017). Case study observational research: A framework for conducting case study research where observation data are the focus. *Qualitative Health Research, 27*, 1060-1068. doi:10.1177/1049732316649160

Morgeson, F. P., Mitchell, T. R., & Liu, D. (2015). Event system theory: An event-oriented approach to the organizational sciences. *Academy of Management Review, 40*, 515-537. doi:10.5465/amr.2012.0099

Morse, J. M. (2015). “Data were saturated . . .”. *Qualitative Health Research, 25,* 587-588. doi:10.1177/1049732315576699

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

Mossburg, E. (2015). A deeper look at the financial impact of cyberattacks. *Financial Executive, 31,* 77-80. Retrieved from http://daily.financialexecutives.org/

Munkhdorj, B., & Yuji, S. (2017). Cyberattack prediction using social data analysis. *Journal of High Speed Networks, 23,* 109-135. doi:10.3233/JHS-170560

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

Nkwake, A., & Morrow, N. (2016). Clarifying concepts and categories of assumptions for use in evaluation. *Evaluation & Program Planning, 59,* 97-101. doi:10.1016/j.eva;progplan.2016.05.014.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-based Nursing, 18,* 34-35. doi:10.1136/ed-2015-102054

Nourian, A., & Madnick, S. (2018). A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet. (2018). *IEEE Transactions on Dependable and Secure Computing, 15,* 2-13. doi:10.1109/TDSC.2015.2509994

Ntalampiras, S. (2015). Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling. (2015). *IEEE Transactions on Industrial Informatics, 11,* 104-111. doi:10.1109/TII.2014.2367322

Omar, M., Mohammed, D., & Nguyen, V. (2017). Defending against malicious insiders: A conceptual framework for predicting, detecting, and deterring malicious insiders. *International Journal of Business Process Integration and Management, 8,* 114-119. doi:10.1504/IJBPIM.2017.083794

Onwuegbuzie, A. J., & Weinbaum, R. K. (2017). A framework for using qualitative comparative analysis for the review of literature. *Qualitative Report, 22,* 359-372. Retrieved from https://www.nova.edu/tqr

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

Patrascu, P. (2018). The appearance and development of national cyber security strategies. *ELearning & Software for Education, 4,* 53-59. doi:10.12753/2066-026X-18-222

Patrascu, P. (2019). Promoting cybersecurity culture through education. *ELearning & Software for Education, 2,* 273-279. doi:10.12753/2066-026X-19-108

Patterson, R. (2015). Silencing the call to arms: A shift away from cyber attacks as warfare. *Loyola of Los Angeles Law Review, 48,* 969-1015. Retrieved from https://digitalcommons.lmu.edu/llr/vol48/iss3/10/

Perrin, A. (2015). *Social media usage: 2005-2015.* Washington, D.C.: Pew Internet & American Life Project. Retrieved from http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

Pham, X. L., Nguyen, T. H., & Chen, G. D. (2018). Research through the app store: Understanding participant behavior on a mobile English learning app. *Journal of Educational Computing Research, 56,* 1076-1098. doi:10.1177/0735633117727599

Pollard, T., & Clark, J. (2019, January). Connected aircraft: Cyber-safety risks, insider threat, and management approaches. *Proceedings of the 52nd Hawaii International Conference on System Sciences.* Retrieved from https://scholarspace.manoa.hawaii.edu/bitstream/10125/59759/0319.pdf.

Pratima, B., Smith, W., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal, 61,* 1189-1195. doi:10.5465/amj.2018.4004

Qu, T., Thürer, M., Wang, J., Wang, Z., Fu, H., Li, C., & Huang, G. Q. (2017). System dynamics analysis for an Internet-of-Things-enabled production logistics system. *International Journal of Production Research, 55,* 2622-2649. doi:10.1080/00207543.2016.1173738

Rid, T., & Buchanan, B. (2015). Attributing cyberattacks. *Journal of Strategic Studies, 38,* 4-37. doi:1080/01402390.2014.977382

Rimando, M., Brace, A. M., Namageyo-Funa, A., Parr, T. L., Sealy, D., Davis, T. L., . . . Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *Qualitative Report, 20,* 2025-2036. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss12/8

Ring, T. (2015). Feature: The enemy within. *Computer Fraud & Security, 2015,* 9-14. doi:10.1016/S1361-3723(15)30111-1

Rivers, A. M., Rees, H. R., Calanchini, J., & Sherman, J. (2017). Implicit bias reflects the personal and the social, *Psychological Inquiry, 28,* 301-305, doi:10.1080/1047840X.2017.1373549

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2,* 121-135. doi:10.1093/cybsec/tyw001

Rosenthal, M. (2016). Methodology Matters: Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning, 8,* 509-516. doi:10.1016/j.cptl.2016.03.021

Rothrock, R., Kaplan, J., & van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59,* 12-15. Retrieved from https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cybersecurity strategies: Global trends in cyberspace. *International Journal of Computer Science and Software*

Engineering, 5, 67-81. Retrieved from https://ijcsse.org/published/volume5/issue5/p1-V515.pdf

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

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., & Bartlam, B., . . . Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity, 52,* 1893-1907. doi:10.1007/s11135-017-0574-8

Schackelford, S. (2016). The intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate risk. *Chapman Law Review, 19,* 445-481. Retrieved from http://digitalcommons.chapman.edu/chapman-law-review/vol19/iss2/5

Scherzinger, G., & Bobbert, M. (2017). Evaluation of research ethics committees: Criteria for the ethical quality of the review process. *Accountability in Research: Policies & Quality Assurance, 24,* 152-176. doi:10.1080/08989621.2016.1273778

Shaw, J. D., Bansal, P., & Gruber, M. (2017). From the editors- new ways of seeing: Elaboration on a theme. *Academy of Management Journal, 60,* 397-401. doi:10.5465/amj.2017.4002

Sibi Chakkaravarthy, S., Sangeetha, D., Venkata Rathnam, M., Srinithi, K., & Vaidehi, V. (2018). Futuristic cyberattacks. *International Journal of Knowledge Based Intelligent Engineering Systems, 22,* 195-204. doi:10.3233/KES-180384

Siegner, M., Hagerman, S., & Kozak, R. (2018). Going deeper with documents: A systematic review of the application of extant texts in social research on forests. *Forest Policy & Economics, 92,* 128-135. doi:10.1016/j.forpol.2018.05.001

Simmons, R. (2016). The failure of the Computer Fraud and Abuse Act: Time to take an administrative approach to regulating computer crime. *George Washington Law Review, 84,* 1703-1724. Retrieved from http://www.gwlr.org/

Slota, G. M., & Madduri, K. (2015). Parallel color-coding. *Parallel Computing, 47,* 51-69. doi:10.1016/j.parco.2015.02.004

Smrithy, G. S., Cuzzocrea, A., & Balakrishnan, R. (2018). Detecting insider malicious activities in cloud collaboration systems. *Fundamental Information, 161,* 299-316. doi:10.3233/FI-2018-1704

Solanki, R., & Singh, H. (2015). Efficient classes of estimators in stratified random sampling. *Statistical Papers, 56,* 83-103. doi:10.1007/s00362-013-0567-1

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36,* 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Spalević, Ž. (2014). Cyber security as a global challenge today. *Singidunum Journal of Applied Sciences,* 687-692. doi:10.15308/SInteZa-2014-687-692

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92,* 178-188. doi:10.1016/j.future.2018.09.063

Starr, M. (2014). Qualitative and mixed methods research in economics: Surprising growth, promising future. *Journal of Economic Surveys, 28,* 238-264. doi:10.1111/joes.12004

Sullivan, R. J., & Maniff, J. L. (2016). Data breach notification laws. *Economic Review, 101*, 65-85. Retrieved from http://www.kansascityfed.org/publications/research/er/

Tracy, S. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative Inquiry, 16*, 837-851. doi:10.1177/1077800410383121

Tran, J. L. (2015). Navigating the Cybersecurity Act of 2015. *Chapman Law Review, 19,* 483-499. Retrieved from http://digitalcommons.chapman.edu/chapman-law-review

Trotter, R., & Chythlook, A. (2016). High-frequency trading and internet crime: One cannot trust the screen. *Journal of Financial Service Professionals, 70,* 81-88. Retrieved from https://www/financialpro.org/pubs/journal_index.cfm

Trudel, R., Murray, K. B., Soyoung, K., & Shuo, C. (2015). The impact of traffic light color-coding on food health perceptions and choice. *Journal of Experimental Psychology Applied, 21,* 255-275. doi:10.1037/xap0000049

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C. (2017). Some guidance on conducting and reporting qualitative studies. *Computers & Education, 106,* A1-A9. doi:10.1016/j.compedu.2016.12.002

Uprichard, E., & Dawney, L. (2019). Data diffraction: Challenging data integration in mixed methods research. *Journal of Mixed Methods Research, 13,* 19-32. doi:10.1177/1558689816674650

van der Vegt, G. S., Essens, P., Wahlstrom, M., & George, G. (2015). Managing risk and resilience. *Academy of Management Journal, 58,* 941-980. doi:10.5465/amj.2015.4004

van Knippenberg, D., Dahlander, L., Haas, M., & George, G. (2015). Information, attention, and decision-making. *Academy of Management Journal, 58,* 649-657. doi:10.5465/amj.2015.4003

Viuker, S. (2014). Cyber security still more reactive than proactive. *Banking New York, 34*, 20-22. Retrieved from http://www.bankingny.com/portal/

von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal, 15,* 407-426. doi:10.2307/255139

Voris, J., Song, Y., Salem, M. B., Hershkop, S., & Stolfo, S. (2018). Active authentication using file system decoys and user behavior modeling: Results of a large scale study. *Computers & Security, 13*(2), 1-13. doi:10.1016/j.cose.2018.07.021

Wahyudi, A., Kuk, G., & Janssen, M. (2018). A process pattern model for tackling and improving big data quality. *Information Systems Frontiers, 20,* 457-469. doi:10.1007/s10796-017-9822-7

Wallace, M., & Sheldon, N. (2015). Business research ethics: Participant observer perspectives. *Journal of Business ethics, 129,* 267-277. doi:10/1007/s1055-01402102-2

Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information, 6,* 183-211. doi:10.3390/info6020183

Ward, K., Gott, M., & Hoare, K. (2015). Participants' views of telephone interviews within a grounded theory study. *Journal of Advanced Nursing, 71,* 2775-2785. doi:10.1111/jan.12748

Watts, L. L., Todd, E. M., Mulhearn, T. J., Medeiros, K. E., Mumford, M. D., & Connelly, S. (2016). Qualitative evaluation methods in ethics education: A systematic review and analysis of best practices. *Accountability in Research, 24,* 225-242. doi:10.1080/08989621.2016.1274975

Wee, B. V., & Banister, D. (2016). How to write a literature review paper? *Transport Reviews, 36,* 278-288. doi:10.1080/01441647.2015.1065456

Wirth, N. (2018). Hello marketing, what can artificial intelligence help you with? *International Journal of Market Research, 60,* 435-438. doi:10.1177/1470785318776841

Wolff, J., & Lehr, W. (2017). Degrees of ignorance about the costs of data breaches: What policymakers can and can’t do about the lack of good empirical data. Advance online publication. doi:10.2139/ssrn.2943867

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *Qualitative Report, 20,* 134-152. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss2/12

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Los Angeles, CA: Sage.

Yong-Jun, Z., & Deng-Feng, L. (2016). A new definition and formula of entropy for intuitionistic fuzzy sets. *Journal of Intelligent & Fuzzy Systems, 30,* 3057-3066. doi:10.3233/IFS-152031

Zubiaga, A., Procter, R., & Maple, C. (2018). A longitudinal analysis of the public perception of the opportunities and challenges of the Internet of Things. *PLoS ONE, 13*(12), 1-18. doi:10.1371/journal.pone.0209472

Zureich, D., & Graebe, W. (2015). Cyber security: The continuing evolution of insurance and ethics. *Defense Counsel Journal, 82,* 192-198. Retrieved from http://defensecounseljournal.org/

Appendix: Interview Protocol

The research question guiding the study was as follows: What strategies do IT administrators and airline managers use to reduce the fiscal impact of cyberattacks? The semistructured interviews will take approximately 30-40 minutes each.

Introduction and ensure the participant is comfortable and understands the process.

- Semistructured interviews will be conducted via telephone or face-to-face in a public place. Each audio interview will begin with an introduction, greeting, after advising the participant that the recorder has been turned-on. I will thank participants for their willingness to participate in this study and verify that each participant understands the details as I previously explained, and has retained a hard copy of the approved consent form. I will also advise the participant that I will be recording the interview as follows: "Although I will be recording our conversation, I would like to remind you once again that your answers will be treated as strictly confidential, and your name will not be used as you have been provided a unique numerical identifier." I will ensure that the participant is comfortable with the process and environment and reiterate the participation is voluntary and it is their right to withdraw at any time.

Conduct the semistructured interview

- I will then discuss the interview timeframe as follows: "I estimate that this process should take approximately 30 minutes, however, I have reserved 45 minutes in the event you have questions or would like more time." Participants will be asked the same seven pre-scripted questions and allowed to speak freely.

Probing Questions (3 of 7 pre-scripted questions)

1. What strategies are currently in place to reduce the fiscal impact of cyberattacks?
2. How have cyberattacks affected or altered your department's processes?
3. How do you assess the effectiveness of the strategies you have implemented to reduce cyberattacks?

Implementing member checking

- Before concluding the interview phase, I will answer any additional questions and thank the participants for assisting in this study. I will then review the responses and any public documents provided for document review. For further clarification, each participant will be advised that they may be asked to participate in a brief 20-minute follow-up session. This step will be the member-checking segment in order to allow the participant the opportunity to add, validate, or correct the researcher's summation of the interview.

Protection of Participant Privacy (storage of files)

- Once I have completed the member checking, I will synthesize the information and conclude my study. Upon receiving formal approval from the CAO, I will share the approved copy of the doctoral study with each participant via e-mail. Data will be securely stored in a locked file for a period of 5 years to protect participant's privacy; after-which time, it will be destroyed. Data collection will be conducted in compliance with IRB standards.