MANAGING CYBER DEFENSE AS A BUSINESS THREAT FOR SMALL AND MEDIUM ENTERPRISES

by

Binh Quang Vo

Dissertation

Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

May 2023

Abstract

The U.S small and medium businesses (SMBs) are constantly attacked by cybercriminals. Alarmingly, the number of victimized SMBs is growing considerably every year. This results in the increasing loss of billions of dollars and risks to the national economy. The problem addressed was the rising number of cyberattacks critically harming SMBs resulting in revenue loss, damages to reputation, and business closure. The purpose of this research was to reveal the contemporary barriers and challenges that impact cybersecurity competencies of SMBs. This study used semi-structured interviews of participants who are currently working as cyber professionals in SMBs across industries. The goal of this research study was to reveal elements preventing SMBs from effectively defending against cyberattacks. This study provided a deeper understanding of challenges SMBs face in order to defend their digital infrastructure through experiences of employees currently working in SMBs. The findings revealed thirteen themes addressing both organizational and technical challenges of SMBs in fighting against the vicious cyberattacks. In addition, in the thirteen themes, there are recommendations that participants suggested SMBs should implement to mitigate cyberattacks. This research study offers breakthrough information to cyber professionals, businesses, business leadership, educators, cybersecurity vendors, and researchers.

Key words: cybersecurity, business, IT professionals, vulnerability, cybercrime.

MANAGING CYBER DEFENSE AS A BUSINESS THREAT FOR SMALL AND MEDIUM ENTERPRISES

by

Binh Quang Vo

Dissertation

Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

May 2023

Approvals

_____	_____
Binh Vo, Doctoral Candidate	Date
_____	_____
Mike D. Kipreos, DBA, Dissertation Chair	Date
_____	_____
Kimberly Jones, PhD, Committee Member	Date
_____	_____
Edward M. Moore, PhD, Director of Doctoral Programs	Date

Dedication

To GOD: You are my source of wisdom and knowledge. You are the guidelines for my life to be lived in good and righteousness. To FAMILY: You are my strong pillar and strength to persist through most challenging life endeavors. Your sacrifices and dedication nourish and prepare me to achieve greatness in life. To THE UNITED STATES OF AMERICA: You assure the freedom and the dignity of an individual more than any other place on earth that gives me the opportunity to strive and accomplish unthinkable goals. You are my inspiration and the last best hope on earth for me and my family. Dedication to God, family, and my beloved country.

Acknowledgments

I would like to thank my magnificent dissertation chair, Dr. Mike Kipreos, for the exceptional support, encouragement, and guidance through every single challenge both in the dissertation process and in life. Thank you for pushing me forward to achieve my educational goal, especially through the hardest time of my life and academic career when I attempted to quit. You are very understanding and supportive to the level that I feel very comfortable sharing my daily hardship with you. I am grateful for your professionalism and compassion.

I also wish to acknowledge Dr. Sabrina Rood, who strived very hard to make my writing as close to perfection as possible. Your support and work in the last four years have been remarkable to my achievements.

I would also like to extend a special thanks to Christopher Richins and Justin Henry. You are not friends but brothers who help me integrate into the American ways of life. You constantly remind me of the direction I should follow to achieve excellence. The research topic of this study was inspired by both of you 8 years ago. On top of that, your insights were a major part of the success of this research. I am blessed to have both of you in my life.

The goal of this research study could not have been accomplished without the generous sharing of the seven participants. You opened up about challenges at work and personal experiences in the field of business and cybersecurity. This made the research study possible.

There have been countless sacrifices made by my family supporting me through this process. You supported me morally, economically, and spiritually. You went above and beyond the definition of sacrifice so that I can accomplish the highest level of education. I love all of you and I look forward to striving my best to make you proud!

Table of Contents

List of Tables

List of Figures

Managing Cyber Defense as a Business Threat for Small and Medium Enterprises

Section 1: Foundation of the Study

The outgrowing number of cyberattacks against the private sector has devastated many businesses, resulting in billions of dollars in losses (Shoemaker et al., 2019). By 2021, the estimated cost of cybercrime is estimated to reach $6 trillion. Importantly, while the issues of cybersecurity in U.S. enterprises are closely examined by researchers and cyber professionals, cyber breaches in U.S. small and medium businesses (SMBs) are often neglected (Kaušpadienė et al., 2019). In fact, small and medium enterprises are victims of 72% of all cyber breaches on U.S. businesses (Fielder et al., 2016). Because U.S. SMBs are the backbone of the national economy and the foundation for national security, this qualitative research study explored and analyzed the problems of cybersecurity impacting business.

This section provides the foundation of the present study on cyber defense in U.S. small and medium business. To begin, the background of the problem will provide the context of this study, with respect to identifying issues and real-world challenges leading to the problem of U.S. businesses continuing to fall victim to cyberattacks. In addition, the problem statement, with general and specific problem, will be presented to illustrate the gap between existing literature and current business practice. Following the problem statement, the purpose statement describes the focus of this study and its design. Related to the purpose statement, the nature of the study discusses the method and design of this research and the rationale for choosing specific types. Importantly, research questions with overarching concepts that guided the direction of this study will be presented. As followed, the conceptual framework proposes three concepts tied to cybersecurity and the business field. Next, the significance of the study, with reduction of gaps, relationship to field study, and biblical integration will be discussed. As well, the definition of

terms describes terms that might not be well known to readers. Then, assumptions, limitations, and delimitations are provided. A comprehensive literature review focusing on cyberattacks, cyber defense, and conceptual frameworks finishes this section on the foundation of the study.

Background of the Problem

Despite excessive investments, the latest security countermeasures, and costly cyber incidents, small and medium businesses continue to be the prime target for cyberattacks that have caused unmeasurable damages to their organizations (Wang, 2019). In fact, 60% of all reported cyber incidents in the U.S. private sector are from SMBs (Hewes, 2016). Hewes (2016) predicted that U.S. SMBs are expected to see a 26% increase in cyberattacks in the near future. Therefore, the cybersecurity and business fields must address the increasing cyber victimization of U.S. SMBs. Given the current antagonistic state of cybersecurity in SMBs, this study sought to extensively explore the problem of the growing number of cyberattacks severely threatening SMBs.

With the existence of cyberspace comes the need for cybersecurity. Since the boom of the Internet in the 1990s, cyberattacks have propagated exponentially, as attacking via the cyberspace is highly profitable and mostly anonymous for attackers (Smith et al., 2019). In fact, 96% of cyberattacks against SMBs are financially motivated, while organizations' poor understanding of security, ineffective deployment of defense mechanisms, and organizational and technical barriers result in more than 90% of compromises (Schiavone et al., 2014). Additionally, besides revenue loss, business reputation is dramatically devastated, which causes long-term and, in some cases, unrestorable destruction to small and medium enterprises, jeopardizing their ability to recover (Morse et al., 2018). In the aftermath of a cyberattack, a company may suffer from any of the following: degraded employee morale, decreased market

valuation, loss of shareholders, declined stock price, and dysfunctional integrity (Smith et al., 2019).

In an effort to explore the uncontrollable widespread increase in the number of cyberattacks against SMBs, researchers have attempted to gain insight into this contemporary business problem. Nevertheless, the majority of current researchers approach the topic of cybersecurity in business with merely two dichotomies (Donalds & Osei-Bryson, 2019). These two dichotomies are technology-assisted attacks and technology-focused attacks. As a result, these dichotomies disregard organizational structure, administrative elements, and nature of the victimized SMBs. Given this significant gap, this study attempted to explore the problem of SMBs continuing to fall victim to cyberattacks from both technical and organizational perspectives.

Problem Statement

The general problem addressed was the escalating number of cyberattacks in the private sector resulting in losses of billions of dollars annually that threatens the stability and growth of the U.S. economy (Bernardo, 2015; Osawa, 2017; Paul & Wang, 2019). The average cost of cybercrime per company is $8.6 million resulting from business interruption, damaged equipment, and loss of data and revenue (Stanciu & Tinca, 2017). Unfortunately, according to Denning and Denning (2016), the current reports and findings about cyberattacks and vulnerabilities in the private sector are significantly limited and ineffective, as enterprises are not fully aware of the possible cyber catastrophe that could cause unrecoverable damage to SMBs across industries. More importantly, SMBs are being attacked more frequently than large-sized firms (“SMBs Are a Huge Target for Hackers,” 2017). With the lack of existing reports and findings about cybersecurity, the recommended approach was to examine the ongoing problem

of cyberattacks in businesses starting from barriers for cybersecurity improvements and challenges for implementing security mechanisms and organizational strategies (Borum et al., 2015; Kure & Islam, 2019; Miraglia & Casenove, 2016; Taitto et al., 2018; Zweighaft, 2017). The specific problem addressed was the growing number of cyberattacks critically threatening SMBs of the U.S. private sector resulting in revenue loss, damages to reputation, and business closure (Paoli et al., 2018; Tagarev et al., 2017).

Purpose Statement

The purpose of this qualitative research was to reveal the contemporary barriers and challenges that impact the latest cybersecurity competencies of small and medium enterprises, through a study of the perception and experience of these organizations regarding cyber defense as a business risk. This study explored the increase of cyberattacks based on technical factors and organizational elements, considering that the effectiveness of cybersecurity requires both technology and business strategies (James, 2018). The research focused specifically on SMBs in the U.S. private sector with fewer than 250 employees. The main objective was to identify the impacts of technical barriers, business strategy, and organizational elements causing cyber vulnerabilities that may result in SMBs becoming cyber victims. Therefore, the cyber-defense capabilities of SMBs were the primary focus of this study. Because existing studies approach the issues of cyberattacks in the business field with either technology-assisted attacks or technology-focused attacks (Donalds & Osei-Bryson, 2019), this study fulfills the gap in both cybersecurity and business fields by adding the human factor and organizational effectiveness elements to the existing body of knowledge. The end goal is to provide SMBs with breakthrough information that could initiate changes in their organizations to defend against the ever-increasing number of cyberattacks in the business sector.

Nature of the Study

The nature of the study section discusses in great detail the research method and design selections for the study. First, the first component of the nature of the study will address the three research methodologies, quantitative, mixed, and qualitative methods, as well as the determining factors for the selected methodology for the study. Second, the discussion of research design will review five research designs: narrative, phenomenology, grounded theory, ethnography, and case study. This section will also give a detailed description and weaknesses of each research design. Then, a thorough explanation for the selected research design for this study will be provided. The objective of the nature of the study was to establish a solid foundation for the strategies and processes to reveal new findings and create a better understanding of the ongoing problem of cyberattacks against U.S. business.

Discussion of Research Method

Quantitative. Quantitative research is designed to collect structured and statistical data to provide empirical results or evidence by testing hypotheses and objectivity (Creswell & Creswell, 2017). As a result, this method is highly effective in determining relationships and performance measures. In terms of the application of quantitative methods in solving business problems, business professionals from across various industries rely more on quantitative research (76%) than qualitative research (10%) or mixed research (14%) (Cameron & Molina-Azorin, 2011). Nevertheless, weaknesses in the nature of quantitative methods are a concern for researching cybersecurity in business, such as reductionistic approach and concise and narrow focus. One reason for this is that quantitative research methods exclude organizational cultures, relationships, and emotional conditions of participants (Collins & Cooper, 2014). In addition, findings of quantitative research do not consider human-factor issues such as “credibility,

dependability, transferability and confirmability" (Sinkovics et al., 2008, p. 689), which could be utilized to effectively embrace the attitudes and ideals of stakeholders with respect to cybersecurity in business. As a result, quantitative research methods are not appropriate for exploring the perception and experience of businesses in defending their organizations against cyberattacks.

Mixed Methods. Mixed methods are a combination of qualitative and quantitative methods. Mixed methods provide researchers a unique approach to their studies because the features and characteristics of both quantitative and qualitative methods are included in the research process (Schoonenboom & Johnson, 2017). Theoretically, mixed methods could fill the conceptual gap of both quantitative and qualitative methods because these methods are highly useful in helping researcher and readers in understanding contradictions between qualitative findings and quantitative results (McKim, 2017). In addition, the use of mixed methods offers the flexibility and adaptability for researcher through employing approaches from both quantitative and qualitative methods. With the increasing complexity of business problems, management demands a comprehensive approach that is highly reliable in solving real-world problems while providing a realistic solution. As a result, mixed methods are rapidly gaining more acceptance (Cameron & Molina-Azorin, 2011). Nevertheless, the application of mixed methods in the business field is considered risky because most researchers mistakenly identify the wrong type of research and the interdependency of qualitative and quantitative components (Schoonenboom & Johnson, 2017). Because cyber defense is a contemporary challenge for businesses, researchers studying this topic can ill afford to err in the research method selection process. Therefore, mixed methods are not typically utilized for exploring issues of cybersecurity in small and medium enterprises.

Qualitative. Qualitative methods are oriented toward exploration and explanation, while being subjective with research purposes (meaning and interpretation) and procedures (Creswell & Creswell, 2017). This unique nature allows the researcher to focus on gaining the depth and exploring the richness of a given study with a holistic and naturalistic approach. In fact, there are two main advantages for researchers utilizing qualitative methods in the business environment. These advantages are uncovering "new aspects affecting security operations" and presenting "context-driven insights" to analysts and managers working in companies (Nyre-Yu et al., 2019, p. 438). Additionally, the use of qualitative methods allows small and medium enterprises to share their cybersecurity experience with researchers in a more meaningful way than other methods (Kabanda et al., 2018). Using qualitative methods is the most appropriate approach for the researcher to reveal the current challenges and barriers impacting cybersecurity competencies of participants through exploring their perception and experience regarding cyber defense as a business risk. Therefore, this study employed qualitative methods to analyze small and medium companies.

Discussion of Research Design

Narrative. As the name suggests, narrative design focuses on the experiences of individuals through their lives and stories (Creswell & Poth, 2018). This research design prioritizes concrete events of participants' experience, "rather than focusing on constructs, opinions, or abstractions" (Carless & Douglas, 2017, p. 307). In other words, "narrative accounts embrace the particularity and complexity of individual's lived experience" (Carless & Douglas, 2017, p. 307). Therefore, it is suitable for researchers attempting to describe individual experiences through the context of personal stories. This design is widely used in many social

and humanities subjects. There are two approaches for conducting a narrative research study. They are thematic analysis and case-centered approach (Bruce et al., 2016).

Despite the popularity of narrative design in the social science field, researching cybersecurity in business with this type of approach has many obstacles for exploring issues and barriers of cyber defense within private entities. With the nature of this design, researchers depending on "reporting individual experiences and chronologically ordering the meaning of those experiences" (Creswell & Poth, 2018, p. 68) would capture the big picture of cyber-defense capability inaccurately due to distorted information provided by participants. Also, a narrative design study requires researchers to present participant experiences and stories in a manner that public audiences can understand through personal perspectives (Creswell & Creswell, 2017). This causes a problem, as not all public audiences are familiar with the cybersecurity field. Therefore, given these two challenges of this design, researching cybersecurity in business requires a more appropriate approach.

Phenomenology. Phenomenological design is a highly effective way or means to explore and explain the universal essence of participants' lived experiences through reflecting on those experiences and different forms of intentionality (Poulsen & Thøgersen, 2011). Specifically, this design emphasizes the subjective reality and social constructs of participants in order to fully understand their behavior and point of view (Austin et al., 2009; Krathwohl, 2009). Within the phenomenological design, there are two approaches. They are hermeneutic and transcendental. Hermeneutic phenomenology is the systematic reflection of participants' perspectives on the lived experience (van Manen, 2016), while researchers analyze and categorize personal experiences and notions to explore the depth of lived experience in the transcendental approach (Creswell & Poth, 2018).

The phenomenological design has two disadvantages that affect the outcomes of a study. The first disadvantage is finding qualified participants to study and the second is researcher bias. Because the goal is to be able to describe the shared meaning of experiences, finding participants with a specific experience requires extensive time and effort, especially for sensitive research topics. In addition, researchers could mistakenly inject biases and distortion into a given study during the grouping process of participants' lived experiences (Tufford & Newman, 2012). This possibility would lead the study to a wrong conclusion. Given the nature and weaknesses of phenomenological design analyzed, this approach hinders the exploration of the growing number of cyberattacks critically threatening SMBs in the United States.

Grounded Theory. Grounded theory focuses on the generation or exploration of a theory by grounding data from individuals or groups who have experienced some process or action (Creswell & Poth, 2018; Strauss & Corbin, 1997). This type of research design is commonly applied in the fields of management and organizational research (Alammar et al., 2019). Grounded theory design is a highly structured, yet flexible methodology (Chun Tie et al., 2019). As a result, the grounded theory researcher is enabled to "produce or construct an explanatory theory that uncovers a process inherent to the substantive area of inquiry" (Chun Tie et al., 2019, p. 2). Compared to other qualitative designs, the framework of grounded theory is distinctive as it relies on coded data and comparisons of acquired information (Stake, 2010).

While the use of grounded theory could reveal unique patterns, similarities, and categories regarding the universal essence of a research topic, the subjectivity of collected data may lead researchers to challenges in establishing validity and reliability in the research (Creswell, 2013). This means that the outcomes of a grounded theory research can be inaccurate and invalid due to subjective errors from the data collection process. Additionally, during the

process of grounding data to generate or explore a theory, it is very difficult for researchers to detect and prevent their bias, which sways the research outcomes (Creswell & Poth, 2018). As a result, Alammar et al. (2019) indicated that a grounded theory research is a learning curve in which the researcher must be highly adaptive or "even retreat to other qualitative research methods" (p. 241). Therefore, given the weaknesses of grounded theory research design, this qualitative research design was deemed inappropriate for exploring the problems of cybersecurity in U.S. SMBs.

Ethnography. An ethnographic research design is often a choice of social science researchers, specifically in the anthropology field (Creswell, 2013). The ethnographic study focuses on the shared culture of a specific cultural group that behaves in distinct circumstances (Creswell & Creswell, 2017). Researchers employing an ethnographic design conduct empirical fieldwork to explore and compare cultural similarities and differences of a cultural group through data collection techniques such as participant observation and interviews (Creswell & Poth, 2018). For any ethnographic research, there are two approaches. A researcher employing an ethnographic design can take either an emic (inside or folk) or etic (outside or analytic) approach to describing a particular cultural group being studied (Creswell & Creswell, 2017).

Although ethnographic research design is commonly used in the anthropology field, there are many disadvantages for a researcher using this design in the fields of business and cybersecurity. The ethnographic research design has two major weaknesses, which are challenges in defining the spatial and temporal boundaries and difficulty in determining and understanding the context of the study (Hammersley, 2006). Defining the spatial and temporal boundaries is considered highly challenging for a researcher attempting to study a cultural group sharing similar experiences and backgrounds. The main reason is that behaviors of members in

any particular group being studied often change unpredictably, for which defining specific boundaries is nearly impossible (Ayala et al., 2019). Furthermore, employing an ethnographic design requires the researcher to understand the contexts and circumstances of the cultural group (Creswell & Poth, 2018). This requirement means that, for researchers who are outsiders to the cultural group being studied, the research with an ethnographic design will take considerable time and effort to ensure the accuracy of research outcomes (Hammersley, 2006). In short, the best way for a qualitative researcher with an ethnographic design to achieve research goals is to be a member of the group being studied for an extended period of time. Therefore, given the weaknesses of the ethnographic design, the ethnographic design was deemed inappropriate for the researcher to conduct the study on the ever-increasing cyberattacks in U.S. SMBs.

Case Study. This type of research design concentrates on in-depth exploration of one or more cases concerning an individual or a group of individuals within the boundaries of life (Naumes & Naumes, 2012; Yin, 2018). The use of a case study design allows the researcher to determine the what and the why of several events. In addition, the case study design supports the researcher in collecting data and recognizing changes during the research process (Yin, 2018). These characteristics make case study design appropriate for researchers to explore the complexity and richness of a case or set of cases. That intention could be achieved through a collection of measures from carefully identified participants to describe the phenomenon or themes (Bitektine, 2008).

For this study, the researcher chose the application of case study design to explore the complexity and patterns of the contemporary challenges of cybersecurity in businesses. Given that cybersecurity is an emerging field with multiple research gaps, the nature of case study design supported the researcher in capturing the how and why questions of cybersecurity in

companies. Indeed, this research design is considered a powerful tool, allowing researchers to make in-depth and multi-faceted explorations of complex challenges in real-life settings, especially in the fields of business, law, and policy (Crowe et al., 2011). Importantly, the use of case study design provided the researcher with detailed qualitative information and permitted the investigation of otherwise impractical situations. Therefore, case study design was used to effectively explore multiple aspects of cyber-defense issues in U.S. businesses.

Summary of the Nature of the Study

This study employed qualitative method with case study design. With the employment of the qualitative method, this study developed a further understanding than would have been possible using the quantitative design about the contemporary barriers and challenges that impact the latest cybersecurity competencies of U.S. SMBs, through a study of the perception and experience of these organizations regarding cybersecurity as a business risk. Of the narrative, phenomenological, case study, and grounded theory research designs, case study design method provided the most applicable instrument for the researcher to explore the in-depth and multifaceted challenges of cyberattacks in companies. Specifically, case study design supported the researcher to capture the how and why questions of cybersecurity. Thus, the employment of qualitative method with case study design was selected as most suitable for this research.

Research Questions

This study addressed the problem of the growing number of cyberattacks against small and medium enterprises within the U.S. private sector (Paoli et al., 2018; Tagarev et al., 2017). This qualitative study relied on one central research question and sub-questions to explore the connection between cyberattacks and cyber-defense capabilities of small and medium enterprises. The central research question addressed the problem being studied in this research,

which is the ever-increasing number of cyberattacks against U.S. small- and medium-sized businesses. More importantly, there were sub-questions concerning cybersecurity in U.S. businesses. First, these sub-questions focused on several types of challenges restricting business organizations from improving capabilities of their cyber defense. The researcher categorized challenges impeding cyber capabilities of companies into two categories: technical and organizational. Second, there were sub-questions attempting to explore mitigations for the problem of U.S. SMBs increasingly falling victim to cyberattacks. The mitigations that were explored by sub-questions focused on cybersecurity and organizational mechanisms.

The central research question and sub-questions were:

RQ1. Why do small- and medium-sized businesses increasingly fall victim to cyberattacks?

RQ1a. What are the existing types of barriers that impede enterprises from improving cybersecurity capabilities?

RQ1b. How impactful are organizational barriers on small and medium enterprises in improving their cybersecurity capability?

RQ1c. How impactful are technical barriers on small and medium enterprises in improving their cybersecurity capability?

RQ1d. What are the practical cybersecurity mechanisms that could boost the cyber-defense capabilities of small- and medium-sized businesses?

RQ1e. What are the practical organizational mechanisms that could boost the cyber-defense capabilities of small- and medium-sized businesses?

Conceptual Framework

This qualitative study explored the contemporary problem of SMBs continuously being targeted and victimized by cyberattacks. With this in mind, theories that address both the cybersecurity field and the business field were the most appropriate for use in this study. More importantly, the appropriate theories for this study were those that cover both technology and organizational elements of the problem of the ever-increasing cyberattacks against U.S. SMBs. There are numerous theories that explore these two fields conjointly. The most relevant theories suitable for this study were the theories of cyber situational awareness (CSA) (Kemper, 2019), cyber defense mechanisms (CDM) (Reagin & Gentry, 2018), and Control Objectives for Information and Related Technology (COBIT) 5 (Sunthonwutinun & Chooprayoon, 2016).

Cyber Situational Awareness Theory

Cyber situational awareness (CSA) is a fundamental theory in the cybersecurity realm, used by public and private entities and other stakeholders to enhance the cyber-defense capability of the organizational decision-making process (Franke & Brynielsson, 2014). The core of cyber situational awareness theory consists of three primary components: detection (level 1), understanding of the situation (level 2), and impact assessment on future (level 3) (Pöyhönen et al., 2019). These components provide the foundation for decision makers in organizations to make accurate conclusions, consider input for decision-making processes, and strengthen evaluation ability with respect to information assurance and digital security. With 90% of cyber breaches resulting from human error, the more unaware that employees are about cyber vulnerabilities, the higher the possibility of cyberattacks against their businesses (Kemper, 2019). The application of cyber situational awareness theory addresses the human factor aspects of risk-causation of cyberattacks. By understanding how employees in SMBs perform at each level of

this theory, this study revealed possible weaknesses in their decision-making processes that may result in vulnerabilities. Correspondingly, attacks caused by human factors were a major concern for participants. They claimed that human factor is the weakest link in any organization's cyber defense. In fact, weaknesses of human factor were a major theme of the data collection. Interestingly, cyber situational awareness was valued considerably by participants as they believed employees with cyber awareness could have limited popular cyber risks. Furthermore, given that 90% of cyberattacks originate from employees' lack of awareness (Kemper, 2019), cyber situational awareness theory was the most effective instrument to investigate challenges and barriers of cyber defense in terms of its non-technical dimensions. Cyber adaptability of several government entities has been greatly enhanced by improving security awareness (Pöyhönen et al., 2019); therefore, this theory is fundamental in the cybersecurity field and the business field. Based on the data analysis, cyber awareness was the fundamental component of many themes. In other words, CSA theory is the essence for the themes of the lack of knowledge, the human factor is the weakest link, security policies, and cultivating an organizational culture for cybersecurity.

Cyber Defense Mechanisms Theory

Cyber defense mechanisms (CDM) theory is a component of cyber deterrence, which focuses on a denial-of-attacks strategy (Ryan, 2018). The rationale for applying cyber defense mechanisms theory in businesses is to discourage attackers in conducting cyberattacks, as the cost/benefit calculus is impacted by defensive mechanisms. There are two approaches to implementing defense mechanisms: passive and proactive. Common passive mechanisms in businesses are anti-virus software, firewalls, and other similar measures. In one study, CDM theory has pointed out that a majority of victimized businesses relied solely on passive measures

and their networks were penetrated in less than 12 hours (Barnes, 2018). Cyber professionals believe that the frequency of cyberattacks against businesses can be reduced significantly when proactive mechanisms are implemented, as this limits the number of threat actors. From the perspectives of both the cybersecurity and business fields, the theory of cyber defense mechanisms serves as the technical framework and standard for private entities in toughening up their defense capability. Applying this theory toward the exploration of the growing number of cyberattacks against small- and medium-sized enterprises addressed the technical aspects of the cyber problem. Unfortunately, participants revealed that many SMBs do not have the technical structure for both passive and proactive mechanisms. They confirmed the benefits the denials-of-attacks strategy and passive defense instruments as addressed by CDM theory. By analyzing CDM theory and collected data, it shows that CDM theory serves greatly as a conceptual frameworks for SMBs to build their defense mechanisms due to the current context of technology in SMBs. CDM theory precisely addressed concerns of participants in various themes. These themes are technology deficiencies, the advancement of technology, the lack of investment in cybersecurity, the obsolete technological infrastructure, and outsourcing cybersecurity.

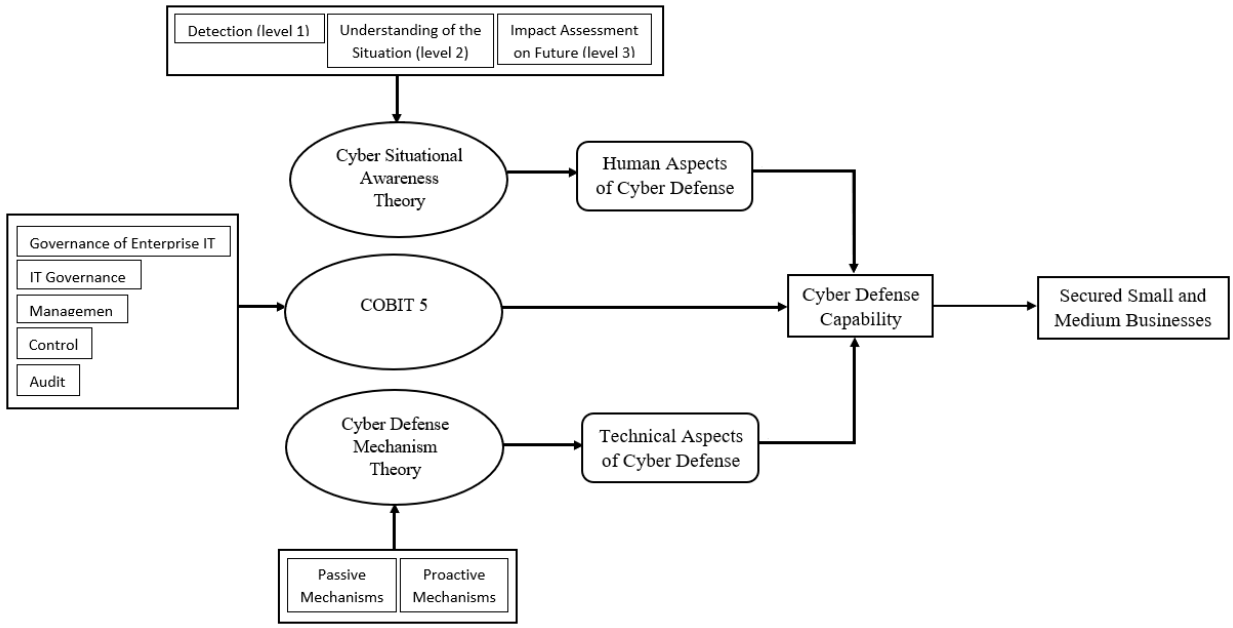
Control Objectives for Information and Related Technology (COBIT) 5

COBIT 5 is a well-known framework serving both the cybersecurity and business fields. In fact, it is the only framework for the governance, internal control, and management of enterprise information technology (Rubino et al., 2017). Many companies are relying on COBIT 5 to develop technology strategies and implement security safeguards. Specifically, decision makers adopt five domains of COBIT 5 for enhancing control environment, internal control system, and risk assessment. The five domains, which cover both technical and non-technical

aspects of an enterprise and its business process, constitute the governance of enterprise information technology (IT), IT governance, management, control, and audit (De Chaves et al., 2011). The application of COBIT 5 is vital to all businesses across industries as technology is the foundation for cybersecurity, operation, production, and strategy. Therefore, this framework was the strategic tool that exposed the strengths and weaknesses of SMBs in securing their infrastructure and assets in the cyberspace. Under the lens of COBIT 5, governance, compliance, IT operations, security and risk management, and IT audit and governance of business were examined meticulously (Alkhaldi et al., 2017). Because COBIT 5 is the conceptual bridge between the fields of cybersecurity and business, this study of the ongoing problem of growing cyberattacks in small and medium enterprises depended greatly on its components in order to explore both human factors and technical challenges of the current situation. While COBIT 5 covers comprehensively vital components of business cybersecurity, only a few components of COBIT 5 applied to the current circumstances of security in SMBs, as revealed by participants. COBIT 5 addressed in detail many components for a strong IT infrastructure. However, SMBs do not have the elements that COBIT 5 addresses. For example, based on collected data, having a strong cybersecurity team in a company is almost non-existent, therefore, having that team conducting IT audit is non-applicable in the context of SMBs. Nevertheless, COBIT 5 set clear guidelines for management to build and protect digital assets. Therefore, COBIT 5 serves as a model for SMBs to upgrade strategically and manage effectively.

Figure 1

The Application of CSA, CDM, and COBIT 5 in Strengthening Cyber-Defense Capability of Businesses



Summary of the Conceptual Framework

The researcher designed the conceptual framework shown in Figure 1 to illustrate how cyber situational awareness theory, cyber defense mechanisms theory, and COBIT 5 interact with one another in strengthening cyber-defense capability of businesses. Conceptual frameworks exploring a problem in these two fields must be comprehensive and effectual to expose the issues of participants in detail. They not only cover both technical and non-technical aspects of cyberattacks but also all of the components and organizational levels of businesses. Specifically, cyber situational awareness targets vulnerabilities caused by employees' negligence that make businesses become easy targets for threat actors. It addresses human factors, training

programs, and organizational implementation. Cyber defense mechanisms theory focuses on the technical dimension of businesses, with respect to improving cyber-defense capability and deterring threat actors. Additionally, COBIT 5 strengthened this study by uncovering flaws in cyber defense of SMBs with five components that comprehensively cover all areas of an enterprise. With these three powerful frameworks, this study revealed the contemporary barriers and challenges impacting cyber-defense capabilities that have allowed businesses to continue to fall prey to cyberattacks.

Definition of Terms

Terms are critical to understand the significance and objectives of this study. This definition of terms helps readers to better understand the research study. Technical and ambiguous terms commonly used in cybersecurity and business fields are defined. More importantly, these terms are the latest specialized terminologies used in both cybersecurity and business fields. Below are terms listed and defined in alphabetical order.

Advanced Persistent Threat (APT):

A cybersecurity vulnerability that enables a threat actor to gain unauthorized access and stealthily control over an organization's system for an extended period without awareness of the network owner (Bahtiyar, 2018).

Backdoor:

Backdoor is a means for cyber perpetrators to negate authentication procedures and bypass security mechanisms to access information systems or encrypted data (Singh Kunwar et al., 2018). Attacks enabled by backdoor are often related to software and databases of the victimized business (Dai et al., 2019).

Business Continuity Planning (BCP):

The administrative procedures prepare for and maintain business activities following disruption and disaster to mitigate both internal and external risks (Fisher et al., 2017).

Compromised Systems:

Describing a computer network of an organization that has been maliciously broken into by threat actors without the administrators' awareness (Khosroshahy et al., 2013). In cybersecurity, compromised systems are often associated with botnet attacks.

Cybersecurity Awareness:

Understandings with attitudes and behaviors that assist an organizational structure in protecting computer systems and information assets (Li et al., 2019). Cybersecurity awareness typically focuses on preventing cyber threats.

Defense in Depth:

A strategy of cyber defense that relies on a collection of defensive mechanisms to defeat attacks on networks and systems (Cleghorn, 2013).

Distributed Denial of Service Attack (DDoS Attack):

A type of cyberattack that disrupts services of information systems by overwhelming network infrastructure with a massive flood of traffic (Hoque et al., 2015).

Internet of Things (IoT):

A system of interdependently interrelated computing devices and digital machines connected to the Internet with the capability of collecting and exchanging data (Boyes et al., 2018).

Pen-testing:

A simulated cybersecurity assessment attempts to reveal and analyze the vulnerability and capability of a network to provide gaps in cyber defense (Goel & Mehtre, 2015).

Assumptions

In qualitative research, assumptions are presumed facts that are believed to be true (Marshall & Rossman, 2016). To accurately research the ongoing problem of growing cyberattacks in small and medium enterprises, participants must possess the proficient knowledge and experience with their organization's cyber-defense mechanisms and organizational factors required in order to provide accurate and valuable responses (Rajivan & Cooke, 2018). Importantly, there was an assumption that each participant was truthful in depicting his or her personal opinions and not those of another regarding the provided situations. To provide a safe environment for participants to express their true opinions, specific parameters were taken to ensure that anonymity and confidentiality were preserved for each participant (Leedy & Ormrod, 2013). Response bias is a foreseeable risk for this assumption, as participants may have responded inaccurately to cover organizational weaknesses and cyber vulnerabilities. This bias is caused by the sensitive nature of the cybersecurity field, for which participants may feel they weaken their organizations by providing details of cyber-defense vulnerabilities and organizational information (Rajivan & Cooke, 2018). Responses might skew the accuracy of data collection. The risk of response bias was mitigated with carefully constructed questions and ensuring the anonymity of respondents (Dodgson, 2019; Jamshed, 2014). Finally, by collecting data from participants working in various cybersecurity and IT roles, the researcher assumed that the collected responses revealed the complexity and patterns of the research problem that leads to

new theories addressing businesses increasingly falling victim to cyberattacks (Rajivan & Cooke, 2018).

Limitations

Many limitations have the potential to constrain the research process; however, for the purpose of this qualitative case study, there were two potential limitations that were addressed in conjunction with mitigation efforts that were utilized. The foremost limitation of the research was that there is limited preexisting literature addressing cyber-defense capabilities of U.S. SMBs. Therefore, there is a gap in the existing knowledge and core themes of the cybersecurity field (Dawson, 2018). This limitation was somewhat mitigated with the application of the case study design, which supported the in-depth and detailed examination of cybersecurity in businesses. The last limitation, due to the nature of qualitative research, is that the study results might have been unintentionally influenced by the researcher during the process of data analysis and interpretation (Creswell & Poth, 2018). This risk was mitigated by strictly following data analysis procedures and valuing all responses equally.

Delimitations

This study focused exclusively on participants from specifically sized and geographically located business entities. Selected participants in this study were employees currently working in cybersecurity and information technology roles in businesses located in the United States. The main preference was employees directly involved with the cyber-defense capability of their business organizations. Specifically, seven employees from both genders participated in this study. The age range of participants was from 25 to 65 years.

Significance of the Study

A cyber catastrophe will undoubtedly destroy economies and infrastructures of multiple countries because they are virtually linked and dependent on each other in cyberspace (Kim, 2018). Specifically, a business victimized by cyberattacks will weaken other organizations in its business network due to the interdependent relationship between companies in a business network (James, 2018). The damage in prediction is likely true as, on the national level, cyberattacks already cost the U.S. private sector billions of dollars annually. Therefore, this study will contribute to stopping the predicted cyber catastrophe, starting from addressing the rising number of cyberattacks against U.S. businesses. Specifically, this research reduces the gaps between the fields of cybersecurity and business, establishes the ethical ground based on Christian values and principles, and explores in depth the technology and cyber vulnerabilities in U.S. businesses.

Reduction of Gaps

Due to the continuous growth in business and cybersecurity, perpetual gaps exist relating to cyber defense in commerce. As a result, there are always gaps that need to be explored and studied, to provide cyber professionals and business decision makers with the latest landscape of cyber defense in commerce. These gaps promote a deficiency in knowledge and an abundance of uncertainty, thereby significantly impacting the decision-making process of stakeholders and promoting the increase of cyberattacks in recent years (Sallos et al., 2019). In order to deter the success of cyberattacks, new studies are needed every year to identify existing problems of cybersecurity in business and to keep pace with the continuously growing gaps generated by new technology and business trends. For these reasons, the results of this study will reduce the gaps by revealing the contemporary barriers and challenges impacting the cyber-defense capability of

small and medium enterprises. The existing literature addressing cybersecurity in businesses primarily emphasizes technology-assisted attacks and technology-focused attacks, while ignoring other significant elements leading to motivation for threat actors' cyberattacks such as the human factors of stakeholders, organizational structure, business operation, and leadership (Donalds & Osei-Bryson, 2019). Significantly, this study approached the cyberattack problem from both technical and non-technical perspectives to provide a comprehensive picture of the ongoing problem.

Implications for Biblical Integration

God created the field of business as an avenue by which His purposes could be fulfilled. For the purpose of this qualitative study, three purposes were addressed, beginning with that of improving the lives of God's children (Keller & Alsdorf, 2014), promoting interactions and fellowships of His children (1 John 1:17 NIV), revealing human beings' weaknesses and improving them (Act 3:19 NIV). Indeed, business contributes to the betterment of society with products and services, serves as a medium for individuals to interact and collaborate, and improves human flaws with occupational experience and workplace education and training. With these divine purposes, any threat against businesses and its growth must be addressed to advance our Creator's providence. This theological principle is the fundamental philosophy for exploring cyberattacks in this study that are not only depriving businesses of revenue, intellectuality, and growth, but also directly endangering the stability of the society. More than that, the study of businesses falling victim to cyberattacks represents the fight between good and evil. In this fight, cybersecurity is the whole armor of God, for which it will stand against the schemes of the devil (cybercrime) (Ephesians 6:11 ESV).

Relationship to Field of Study

All elements of this study align with both the fields of business and cybersecurity because it explored an ongoing problem of cyber-defense capability as a risk in companies. In 2014, the average cost of cyberattacks is $8.6 million per business (Stanciu & Tinca, 2017) and 90% of compromises are originated from victimized companies (Schiavone et al., 2014). Therefore, not only were the practices, structure, and operation of businesses explored in depth but also the technology and cyber vulnerabilities. In addition, all components of this study, such as frameworks, participants, and implications for change, reside exclusively in the field of business. In other words, this research associates closely with technology, operation, human resources, and development of the business umbrella. Therefore, exploring the ongoing problem of the increasing cyberattacks against U.S. small- and medium-sized enterprises is directly related to the business field.

Summary of the Significance of the Study

In brief, this study focused on cyber defense in businesses, specifically their cyber-defense capability, which contributes significantly to the business field. Particularly, this research reduces the existing gap by focusing on both non-technical and technical dimensions of the problem, instead of technology-assisted attacks and technology-focused attacks. In addition to adding to the body of knowledge, the results of the study will serve as the agent for change for cyber professionals and businesses to implement appropriate strategies. By strengthening cybersecurity, customer loyalty and trust, business reputation, and productivity will be enhanced by more than 89% (“Strong Cybersecurity Helps Businesses to Grow,” 2017). From a theological perspective, cyber defense in business is the fight between good (business growth) and evil (cybercrime), for which God is with those people who put forth light in darkness (Isaiah

5:20; Psalm 37:9). With divine cause and providence, this study shed light on breakthrough knowledge regarding the ongoing problem of cyberattacks in businesses.

A Review of the Professional and Academic Literature

The review of professional and academic literature, presented in this study, addresses two fundamental domains of cybersecurity and three conceptual foundations. Importantly, this review discusses both technical and non-technical components of cybersecurity in businesses. First, the first topic to be addressed is that of cyberattacks, including elements of cost, common types, and threat landscapes. Following the section on cyberattacks, the cyber defense section focuses exclusively on methods and mechanisms to support and improve cyber capabilities in businesses. This section discusses the building of a proactive defense, defense capabilities, risk management, cyber-defense mechanisms, disaster recovery and business continuity, and weaknesses of cyber defense. Finally, the section on theories and principles of cyber defense will examine the conceptual connection between technology and enterprise, in which the improvements of cyber capabilities are discussed in terms of organizational changes, policies, training, and governance in U.S. businesses. Particularly, cyber situational awareness theory, cyber defense mechanisms theory, and Control Objectives for Information and Related Technology (COBIT) 5 were the primary framework of theories and principles of the cyber defense section. In short, this review of the professional and academic literature is a thorough overview of cyberattacks, cyber defense, and relevant theories and principles of cybersecurity in U.S. businesses.

Cyberattacks

Understanding the components of cyberattacks against small- and medium-sized businesses is the foremost step for U.S. SMBs to defend against cyberattacks. In doing so, U.S. SMBs have the capability to recognize adversaries, attack approaches, vulnerabilities in IT

infrastructure, and cyber damages. By reviewing the existing literature on cyberattacks, SMBs will become more informed on the problem of companies continuing to fall prey to cybercriminals. With that intention, this section examines the crucial components of cyberattacks. These components are costs of cyberattacks, common cyberattack methods, and threat landscape with respect to U.S. SMBs.

Cost of Cyberattacks. Cyberattacks have severe impacts on victimized businesses. As reported, U.S. businesses lose billions of dollars to cyberattacks annually (Wang, 2019). Hence, costs are inevitably the dominant aftermath that business victims bear after every cyber breach. Therefore, the impacts of costs in the aftermath of a cyberattack must be analyzed in order to better assess the cyber damages. With that intention, the effects of cyber damages in terms of cost, background of security investments, financial costs, and impacts on reputation and customer trust are discussed.

Background of Security Investments in Small and Medium Businesses. Typically, business investments aim at creating value whereas, with the cyberattack pandemic, cybersecurity investments aim to reduce loss incurred by perpetrators. As SMBs continue to fall victim to cybercriminals (Paoli et al., 2018; Tagarev et al., 2017), the expenses to implement and maintain countermeasures rise persistently. Chronopoulos et al. (2018) indicated that with the new threat landscape, businesses are not only driven to spend a larger security budget but also to invest more proactively. Compared to large organizations with tremendous investment in cybersecurity, SMBs are more vulnerable, due to budget constraints and unskilled cyber human resources (Hawkins, 2017). As a result, 72% of cyberattacks target SMBs (Fielder et al., 2016). The information revealed by Hawkins (2017) and Fielder et al. (2016) is confirmed through data collection. Among other discovered themes, the problems of the lack of investment in

cybersecurity, problems of human resources, and lack of knowledge are greatly endangering SMBs. According to Gordon et al. (2015), the recommended optimal security investment for companies should be 36% of the expected financial losses from cyber breaches. Indeed, with a 10% decrease in security budget allocation in 2017, U.S. firms have suffered greater breaches (Fielder et al., 2018). To mitigate cyber risks, businesses must strengthen two dimensions simultaneously: people and technology. To optimize expenses of SMBs, Krishan (2018) recommended that business decision makers implement strategic business continuity management plans, maintain highly skilled incident response teams with extensive encryption capability, and promote employee awareness and training with security culture as the objective. In fact, awareness, training, and cultivating a cybersecurity culture were considered the strategic solution to curb human errors which lead to many cyberattacks. These themes derived from collected data pointed out that when human errors are limited, cyber criminals will less likely attack a company. Additionally, SMBs should have their own security breach model based on threat landscape, interconnectedness of systems, and past events, in order to allocate an appropriate budget for security measures (Musman & Turner, 2018; Srinidhi et al., 2015). Because a company can only be as strong as its weakest possible target, optimal security investment to enhance defense capability is the significant factor in preventing a company from becoming the next victim of a cyberattack pandemic.

Financial Cost. Financial cost as a consequence of cybercrime is inevitable. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (2018) reported that U.S. SMBs lost $2.7 billion in 2018 and this number is expected to rise in the upcoming years. In an effort to enhance their defense capability, 87% of businesses expect to increase their security budget in the next 3 years, with 10% planning to spend double (“Strong Cyber Security Helps Businesses

to Grow," 2017). Unfortunately, when a breach is identified, it costs SMBs $28,000 instantly, and the cost rises to $105,000 if left unresolved for a week (Kaspersky Lab, 2017). Given the severe financial damage, the future cost will be much larger, as volumes of devices in SMBs increase 55% by 2020. Specifically, the expenses commonly associated with an identified attack are the cost of third-party consultants to investigate and resolve the damage, the cost of repairs and/or replacement of systems and information, reduced revenue during downtime, and possible compensation and litigation costs (Brasington & Park, 2016). The cost of cybersecurity that Brasington and Park (2016) identified corresponds with information revealed by participants. The collected data discovered further that SMBs cannot afford these cost. These expenses illustrate that once becoming a victim of cybercrime, SMBs could end up bankrupted or could take an immeasurable time to recover.

Damages to Reputation and Customer Trust. Victimized businesses suffer not only financial loss but also reputational damage in the aftermath of a cyberattack. When a security breach is made public, the reputation of a company is severely damaged, which leads to immeasurable consequences and unrecoverable damages (Information Systems Audit and Control Association [ISACA], 2019a, 2019b). For SMBs, the non-financial damages are brand value and customer trust (Pharris, 2019). Morse et al. (2018) concluded from victimized businesses that, regardless of organizational size, there is a strong correlation between security breaches and negative stock price movements with long-term fluctuations. Factors affecting this correlation are the erosion of customer goodwill and reduced investor confidence in business leadership. It is important to acknowledge that SMBs will require a longer time with greater effort to recover to pre-attack conditions as compared to large corporations, which have the resources to absorb both financial and non-financial damages of a cybercrime (Heikkilä et al.,

2016). Additionally, to be more secure after falling victim, businesses often modify and implement new security mechanisms. Inevitably, new implementations will somewhat impact the existing business processes and organizational management, which may lead to unfavorable operational effectiveness (Deane et al., 2019). With significant non-financial damages on victimized businesses analyzed, cybercrime against enterprises is horrendous and can put an end to unprepared victims.

Common Methods of Cyberattacks. Analyzing the common types of cyberattacks is to acknowledge the malicious and deliberate attempts by threat actors to breach the information systems of SMBs. As attacks are unpredictable, analyzing common attack methods will greatly help businesses in anticipating future possible cyber breaches. In addition, by analyzing common methods of cyberattacks, businesses will be better informed to develop effective measures to mitigate common threats. This section explores and examines methodologies and approaches of seven typical types of cyberattacks. They are business email compromise, data breach, Distributed Denial of Service attack (DDoS attack), malicious software, phishing, ransomware, and social engineering.

Business Email Compromise. In business email compromise (BEC), threat actors compromise business email accounts through social engineering techniques and technical intrusion, to conduct unapproved transfer of funds (Meyers, 2018). Although BEC is considered to be an old-fashioned cybercrime, financial losses of businesses with compromised emails continue to rise annually (Wilson, 2018). Derouet (2016) reported that in 2014 and 2015, compromised emails cost U.S. businesses $3.1 billion, with 84% of enterprises suffering from this type of cyberattack. Notably, compared to other technology-advanced cyberattacks, conducting BEC requires the least knowledge of technology while the financial reward is high, if

not higher than some technology-dependent attacks ("Major BEC Gang Targets Top Executives," 2018). In essence, there are three most common approaches for this type of cyberattack against organizations with a lack of cyber defense, such as SMBs. They are identity spoofing, homograph domains, and username and private email spoofing (Derouet, 2016). While Derouet argued that businesses should enhance their cyber protection through implementation of technical countermeasures such as domain-keys identified mail, domain-based message authentication, reporting and conformance, and sender policy framework, Zweighaft (2017) believed that the root cause of BEC is the lack of awareness and cyber engagement. Implementation of robust training and proactive prevention programs could create a culture of skepticism as the solution for this dilemma of compromised emails. As BEC is a combination of social engineering and technology-based attack, business decision makers are recommended to rely on both technical and non-technical approaches to mitigate BEC threat (Mansfield-Devine, 2016b). Therefore, it depends on businesses' discretion to limit this cyber threat.

Data Breach. A data breach is a security incident in which a release of sensitive data by an unauthorized person or a member of the victim organization could result in financial loss and other severe consequences (Jackson et al., 2019). In fact, 2017 was an alarming year of reported data breaches in U.S. businesses, with 1,579 million incidents. Despite many tough business policies, technical measures, and government regulations, the volume of leaked information is expected to increase 50% in the next 5 years (Wheatley et al., 2016). Importantly, compared to other types of cyberattacks, leaked data directly impacts consumers and partners of businesses, while these victims are unaware of how they are targeted and exploited (Mikhed & Vogan, 2018). From the standpoint of victimized businesses, besides direct consequences such as fraud and theft enabled by leaked data, their market value and reputation are diminished severely; it

takes these victims years to recover and results in bankruptcy in many cases (Schatz & Bashroush, 2016). Specifically, SMBs are the most vulnerable to data breach due to the lack of technical resources, employee skills, or assurance from internal audit (Rai & Chukwuma, 2016). In fact, this was the concern of the majority of participants. To add to the existing problem, SMBs have far more data breach incidents with higher damages than large corporations; however, this situation is often overlooked by the public and those in the cybersecurity field (Rai & Chukwuma, 2016; "SMBs Are a Huge Target for Hackers," 2017; Tolosa, 2015). Based on the reviewed literature, cyber defense in SMBs needs further close examination, especially data breach, as it could lead to other types of cyberattacks.

Distributed Denial of Service Attack (DDoS Attack). Distributed denial of service (DDoS) attacks are highly disruptive for business operations. This type of attack attempts to take away the network resources of a computer or a system from its users temporarily or permanently through flooding the bandwidth with traffic (Saied et al., 2016). To carry out the attack, DDoS forms botnets of networks comprised of infected devices unknown to their users, to overwhelm the victim's bandwidth. Karoui (2016) concluded that, despite the fact that DDoS is well known to the business world, it is the most dangerous for e-commerce businesses based on risk values, as these organizations rely significantly on the availability of Internet resources. Alarmingly, DDoS attacks grow, on average, 23% per year; 2016 was the year with the largest incidence, which involved more than 152,000 devices against a single enterprise system (Kaur Chahal et al., 2019). Commonly, enterprise systems are attacked at the network/transport layer and application layer, for which they are the Achilles' heel of many computer networks in businesses (Hoque et al., 2015). Vishwakarma and Jain (2020) predicted that, although multiple businesses have changed their network architecture and employed powerful hardware, the possibility of

businesses becoming victims of a DDoS attack is inevitable because Internet of Things (IoT) devices with low built-in security mechanisms will become the massive weapon for flooding bandwidths of targeted networks. Based on this prediction, strengthening cyber defense against DDoS attacks is expected to be a fierce challenge for businesses.

Malicious Software. With the existence of computers comes the threat of malicious software or malware. Malware refers to software with the functionality of causing harm to a user, device, and systems (Nikolopoulos & Polenakis, 2017). A wide variety of malware exists with different destructive capabilities. The most well-known malware causing havoc to businesses includes worms, viruses, Trojan horses, and spyware (Shijo & Salim, 2015). According to the FBI's report on 2019 cybercrime, malware is among the top five types of cyberattacks against SMBs, as cyber-defense mechanisms in these organizations, such as antivirus software and scan and monitor programs, are primitive and outdated against the current propagation of malware (FBI News, 2020). Indeed, this type of cyberattack is a pandemic in both the business field and the cybersecurity field (Miraglia & Casenove, 2016). Furnell and Dowling (2019) reported that the volume of malware targeting businesses increased significantly by 145% between 2016 and 2017. Additionally, they predicted that in a decade there will be an explosion of malware attacks. From a cybersecurity perspective, this type of attack is exceptionally challenging to tackle. Malicious software can facilitate other sophisticated cyberattacks and is highly contagious due to the massive growth of Internet-connected devices (Malatji et al., 2019; Visu et al., 2019). Significantly, this malware pandemic destroying businesses is believed to be unstoppable due to the popularity of Internet-of-Thing (IoT) devices and the practice of bring-your-own-device in businesses (Baillette & Barlette, 2018; Qamar et al., 2019). Participants addressed this issue from multiple perspectives. They believe that this issue is originated from the obsolete information

system, weaknesses of human errors, the lack of security, and the absence of a cybersecurity culture. Given the current impacts of malware on business and its threat landscape, it is only a matter of time before private enterprises are crippled by malicious software.

Phishing. Cybercriminals employing phishing combine both social engineering and technical deception to steal confidential data and financial information (Alsharnouby et al., 2015). Despite numerous advances in automated detection as the strategic security mechanism in businesses, this method is still effective against users with lack of cybersecurity awareness. Resnik and Finn (2018) reported that within the last decade, the direct cost of phishing on U.S. businesses was $3.2 billion, while on average, each business spent approximately $3.77 million per year to tackle phishing attacks. Notably, with new countermeasures, this technology-dependent social engineering tactic employed by attackers is changed drastically to adapt to the new security environment (Aleroud & Zhou, 2017). Alsharnouby et al. (2015) argued that, because users only detect 53% of phishing websites and 79% of legitimate websites, the strategic solution against this technical social engineering attack is user education through training programs. In contrast, Moghimi and Varjani (2016) believed that, by creating a massive Internet banking with string-matching algorithm embedded in search engines and web browsers through third-party services, this traditional cybercrime will be solved with 99.14% detection accuracy. In essence, this approach is based on the perception that human errors are unavoidable; therefore, tackling the issue with technical solutions will eliminate this technology-related social engineering cyberattack. Given these points, although phishing is an old-fashioned type of cyberattack, a combination of both human-centered and technology-related solutions is highly crucial to put an ultimate end to phishing.

Ransomware. Ransomware is an increasingly common method of cyberattack that threat actors rely on to target not only private organizations but also public entities (FBI, 2018). In fact, ransomware schemes are highly profitable, so that traditional cyber thieves are abandoning their old ways to favor this method (Allen, 2017). In essence, ransomware works by denying victims from accessing data or systems that are vital to their organizations' operation (Mansfield-Devine, 2016a). According to the FBI, email attachments and "drive-by" websites are the two most typical ways that devices can become infected with ransomware (FBI News, 2015). With the email attachments method, the malware is attached to an important-looking email, from which the device is infected once the user opens the attached file (FBI, Internet Crime Complaint Center, 2018). More recently, victims are increasingly lured by "drive-by" websites, which carry ransomware and transmit to victimized devices through pop-up windows and deceptive content (FBI News, 2015). Mansfield-Devine (2016a) reported that 44% of businesses had fallen victim to ransomware infection, while 27% of them have been attacked more than once. Notably, that report also indicated that two thirds (65%) of affected businesses paid the ransom. Unfortunately, even if victims pay the ransom, it depends on the cybercriminal's mercy to provide the decryption code (FBI News, 2015). O'Kane et al. (2018) forecasted that, as there is a 600% increase in the ransomware families and the estimated market worth of ransomware is $200 million per annum, this method of cyberattack will not only weaken the Internet but also cripple the financial system by destroying businesses. This prediction is highly plausible, with the rise of cryptocurrency and the growth of IoT creating a target-rich environment for cyberattackers (Wani & Revathi, 2020). Ransomware was discussed by participants in the context of malicious software. Indeed, this type of attack falls into seven discovered themes. These themes are lack of knowledge, problems of human resources, the lack of investment in cybersecurity, the human

factor is the weakest link, training and support, security policies, and obsolete technological infrastructure.

Social Engineering. Social engineering is the art of deceiving exploitable users to target confidential information and critical information systems (Tromble & McGregor, 2019). Importantly, it is highly challenging to combat social engineering, as social engineers prey upon human aspects, the weakest link of cybersecurity (Algarni et al., 2017). To exploit the human element of security in businesses, perpetrators execute four foundational phases, which are research, developing rapport and trust, exploiting trust, and utilizing information (Mouton et al., 2016). Bullée et al. (2018) concluded from studying 74 successful social engineering attacks against SMBs that persuasion principles were utilized in 88% of these cases, with authority and liking as the two most commonly used sub-principles. Alarmingly, perpetrators use social engineering attacks as the gateway for other sophisticated cyberattacks, which are highly undetectable and extremely devastating. Indeed, advanced persistence threat enabled by social engineers costs U.S. businesses approximately $400 billion annually (Al-Matarneh, 2020). Disturbingly, the same report also predicts that cybersecurity budgets of U.S. business will soar by 60% in 2020 with respect to social engineering as the root cause. Specifically, without the reinforcement of social engineering exploitation, BEC, ransomware, deceptive phishing, and zero-day vulnerabilities would not have the deadly capability to infiltrate most victimized businesses (Al-Matarneh, 2020; Auty, 2015; Proof Point, 2019; Rass et al., 2017). Attacks classified as social engineering attacks were discussed thoroughly by participants through theme 6: Human Factor is the Weakest Link. They claimed that because employees are unaware and untrained, therefore, social engineering types of attacks happen. This leads to a relating theme 9: Obsolete Technological Infrastructure. The consensus perspective of interviewees was that there

will always be human errors and the existing technology should be able to prevent these errors enabling attacks. However, the majority of SMBs, as claimed by participants, has the obsolete infrastructure. Therefore, social engineering types of attacks are both common and dangerous. Similar to other cyber threats, threat actors targeting human errors of computer systems evolve contingently on businesses' countermeasures. For a highly aware business environment in a company, social engineering malicious attempts seem to be more innovative and complex, with strategically organized plans (Aldawood & Skinner, 2019). Therefore, social engineering is a long-term problem for cybersecurity in SMBs as threat actors are extremely adaptive to cope with businesses' solution.

Threat Landscape. The threat landscape of cybersecurity consists of the emerging weaknesses and vulnerabilities. Notably, threat actors often exploit emerging weaknesses and vulnerabilities in technology infrastructure to victimized U.S. businesses (Richardson et al., 2019). Because the fields of cybersecurity and business are constantly changing, reviewing the threat landscape of risks and uncertainties will greatly enhance decision-making processes of companies in planning and investing for cyber-defense mechanisms (Anstee, 2015). According to Anstee (2015), when business decision-makers are informed on emerging cyber weaknesses and vulnerabilities, they can make more effective decisions to adapt to the new threat landscape. With that purpose, artificial intelligence (AI), Internet of Things (IoT), skill shortage, the cloud, and state-sponsored attackers are reviewed and examined as the rising threats against cybersecurity in businesses.

Artificial Intelligence (AI). Artificial intelligence (AI) is a growing technology trend, in not only the business field but also the cybersecurity field. AI is the theory and improvement of computer systems with the capability of performing operational tasks that often require

employees' decisions and operation (Norman, 2017). Because of the high productivity, usability, and functionality, more businesses, especially small and medium sized, are adopting AI to cut costs and improve performance results (Ransbotham et al., 2017). In fact, 80% of business decision-makers view AI as the game changer for organization expansion. Nevertheless, despite the convenience that AI provides, cybersecurity is a concern for this growing technology trend. The use of automated machines can undermine the in-place cyber-defense mechanisms with technical accidents, flawed designs, and insider threats (Yampolskiy & Spellchecker, 2016). Even more dangerous, AI systems with self-modifying and self-improving ability magnify digital vulnerabilities in organizations. Particularly, AI is highly vulnerable to malware for which perpetrators targeting confidential data are the main threat actors (Caviglione et al., 2016). Therefore, while AI is considered a revolutionary adoption for many businesses (Schneider & Leyer, 2019), from the perspective of the threat landscape, its opportunities come with vulnerabilities.

Internet of Things (IoT). With cyberattacks on the rise, the use of IoT devices results in a pessimistic threat landscape for an enterprise environment. Because IoT devices are Internet-capable machines with wide interconnectedness, it is challenging to operate security solutions in businesses with respect to usage activities and network management (Safaei Pour et al., 2019). Alarmingly, these devices have low to no built-in cybersecurity capability because their manufacturers focus on competitive landscape (i.e., production cost) and technical constraints. Indeed, attacks via IoT devices have risen significantly within the past several years, especially DDoS attacks in which each of the observed cyber breaches had devices with one of four types of connection with the victimized targets (Stellios et al., 2018). The four common connections are direct connectivity, direct physical connection, direct logical connection, and indirect

connectivity. As cyberattacks enabled by IoT devices are increasing rapidly, Nebbione and Calzarossa (2020) predicted that IoT-based cyberattacks against U.S. businesses will grow by over a quarter by 2025. With the current landscape and future prediction, IoT is becoming a predominant danger to businesses. Relating to IoT, participants believed security policy and network segmentation are the two solutions limiting the intrusion of cyber criminals. Corresponding to the prediction of Nebbione and Calzarossa, cyberattacks enabled by small personal devices against organizational structure were a concern of a majority of participants.

Skill Shortage. With the fast-growing trends and types of cyberattacks against businesses, there is a severe skill shortage to reinforce cyber-defense capability in companies. With 82% of businesses reporting inadequate human resources with respect to security experts, skill shortage is an imminent threat directly tipping the scale of cyber defense and cyber perpetrators (Petruzzelli & Sharma, 2019). This is a much bigger dilemma for small- and medium-sized enterprises than larger businesses, because 31% of cybersecurity professionals are attracted to a well-paid salary while a large majority of new talents prefer positions with growing job opportunity that only corporations offer (Smith, 2018). Caldwell (2013) predicted that if the growth of cyberattacks is steady and under control, it will take at least 20 years to fulfill the cybersecurity-skill gap. Specifically, as of January 2019, the National Initiative for Cybersecurity Education reported that U.S. businesses are facing a shortage of 314,000 cybersecurity workers (Petruzzelli & Sharma, 2019), while only 7% of U.S. top universities have majors or minors in information security (Coppel, 2016). Alarmingly, the current threat landscape of skill shortage is not only a crisis to U.S. businesses but also to national security, as the private sector is highly vulnerable to threat actors, including nation-state sponsored hackers (“Severe Shortage of Cybersecurity Professionals,” 2018). Indeed, skill shortage was discussed thoroughly by all

participants as organizations that these participants working for are understaffed. One participant discussed further that SMBs cannot compete with large corporations in term of talent attraction because of budget and employment advancement opportunities. Given that the deprivation of skills cannot be filled expeditiously, it will not be long before businesses are hacked because of cybersecurity skill shortage.

The Cloud. With advanced collaboration, improved flexibility, and reduced costs, businesses adopt cloud computing to assist their operations and processes, especially SMBs (Tripathi & Nasina, 2017). Specifically, a majority of SMBs uses the public cloud because of the pay-as-you-go cost structure and flexibility. Nevertheless, many vulnerabilities in cloud computing attract threat actors targeting small-scale businesses. In fact, integrity and confidentiality mishaps in the auction process and the migration process of cloud computing have led to major DDoS attacks against businesses (Majhi & Dhal, 2016). In the worst cases, misconfigurations between cloud service providers and host-level security have resulted in attackers gaining control of targeted hosts and undermining network infrastructure. Furthermore, as mobile cloud computing is gaining popularity in SMBs, enterprises expect to suffer from two threats simultaneously: Internet of Things and cloud computing (Er Amandeep, 2017). Er Amandeep (2017) reported that with reliance on mobile cloud computing, insider threats and data breach are the two biggest concerns for businesses. Additionally, there is a deficiency of cybersecurity professionals specializing in cloud computing in both cloud service providers and businesses, which poses a high risk for a large-scale cyberattack targeting the cloud (Yang et al., 2017). With 51.3% of SMBs looking at outsourcing to cloud service providers (Balco et al., 2017) and $1 trillion spending relating to cloud service in the business sector (Vithayathil, 2018), cyberattacks via the cloud will sharply rise due to the target-rich environment, the use of IoT

devices, and severe skill shortage. With the current situation of the cloud in businesses, the predicted threat landscape is highly unfavorable for SMBs.

State-Sponsored Attackers. With the new risk landscape of cybersecurity in businesses, the backgrounds and attack targets of threat actors also change. With free enterprise as the fundamental idea for the market economy, state-sponsored hackers are becoming the new normal for U.S. business (Vincent, 2017). Compared to major corporations with massive defense capability, U.S. SMBs are easier targets, for which web-based attacks are the most common method. Importantly, these state-sponsored perpetrators are changing to IoT devices as companies are adopting them at a rapid pace. Specifically, weaknesses of coding defects, software design deficiencies, and absence of tamper proofing in business IoT devices are the prime target for this rising type of threat actor (Khera, 2017). Past cyber breaches in U.S. corporations caused by state-sponsored attackers have proven that advanced defense mechanisms of well-funded technology infrastructure could not withstand target-specific cyber strikes of dedicated state-level attackers (Conti & Fanelli, 2019). Although state-sponsored attacks against SMBs are not common contemporarily, Conti and Fanelli (2019) predicted that, with the U.S. government underprepared for protecting the private sector and businesses unaware of their vulnerabilities, companies of all sizes across industries will have to deal with a "cyber Pearl Harbor" in the near future (p. 55). Despite the pessimistic future as a result of state-level attackers, it seems that U.S. SMBs have the valuable time to strengthen their defense capabilities to counter the foreseeable digital "Pearl Harbor" on the cyberspace (Conti & Fanelli, 2019, p. 55).

Cyber Defense

Defense capability is crucial for businesses to defend against cyberattacks. The functions of defense capability are not only to mitigate and eliminate effects of a cyber breach but also to safeguard the assets of an organization. With that critical mission, components of cyber defense in SMBs are carefully reviewed to explore and identify vital elements that could be strengthened for more secure defense capabilities. Companies with better cyber-defense capabilities are less likely to be victimized by cybercriminals (Conti & Fanelli, 2009). With the focus on cyber-defense capabilities, this section examines thoroughly the building of a proactive defense, categories of defense capabilities, parts of risk management, types of cyber-defense mechanisms, plans of disaster recovery and business continuity, and the current weaknesses of cyber defense.

Building a Proactive Defense. A proactive defense is considered the most effective approach that supports businesses fending off sophisticated cyberattacks, especially advanced, persistent attacks that are crippling to all sizes of organizations (Huang & Zhu, 2020). The main principle of a proactive defense is to understand threats and take appropriate procedures to counter cyberattacks. More succinctly, companies building a proactive defense must take both technical and organizational approaches to mitigate future cyberattacks (Byres, 2014; Lai & Wu, 2015; Wagner, 2016). By doing so, businesses are better defended against both technical and non-technical cyberattacks. To build a proactive defense, strategizing defense in depth, understanding cyber threats, and performing routine checkups of software and hardware are reviewed thoroughly, as they constitute the core steps of the transformation of cyber defense to be more proactive.

Defense in Depth. Defense in depth is considered the holistic approach to harden both network infrastructure and configuration by adding both technology and human-centered

solutions to multiple layers of cyber defense (Presher, 2015). The rationale behind this strategy is that, because cyberattacks are well planned and quite complex, not a single defense mechanism or methodology can thwart attacks, especially those with high intensity and number. With technology implementation for defense in depth strategy, Byres (2014) recommended for organizations to install hardware and software that focus inclusively on quickly detecting, isolating, and repressing both attacks and threats. The methodology puts up differentiated layers of defense with threat-specific layers of security mechanisms to overwhelm any adversaries (Byres, 2014). In terms of human-centered solutions, improving human–computer interaction for maintaining security is the central point, as technical mechanisms could be bypassed by employee-caused vulnerability (Lai & Wu, 2015; Wolff, 2016). Specifically, password policy, drive-by download, behaviors of non-malicious users, and preventing employees from circumventing security measures are the real-world concerns in the business environment (Lai & Wu, 2015; Wolff, 2016). Similar to information revealed by Lai and Wu (2015) and Wolff (2016), for human-centered solutions, participants encouraged limiting human errors through training and policy and cultivating a cybersecurity culture. The idea is to form employees' habits of safe human-computer interaction. In brief, defense in depth is not only a strategy supporting organizations in building or transforming their cyber defense, but also may serve as a guideline for implementing defense mechanisms and improving human interaction for maximizing the functionality of those mechanisms.

Understanding the Threats. Understanding cyber threats is the first step of proactively defending against cyberattacks. In a business environment, with the understanding of upcoming threats, organizational decision makers would be more motivated to identify the gap in preparedness (Nam, 2019). Importantly, Nam (2019) concluded from studying U.S. SMBs that

there is an enormous gap between perceived threats of cyberattacks and preparedness for cyber defense. Based on collected data, Nam's statement is accurate in the context of SMBs. Participants blamed the lack of preparedness on business leadership as business owners either have a lack of cyber knowledge or do not believe cyberattacks are imminent threats. Because of the changing landscape of cybersecurity, this conclusion means that U.S. businesses will fall victim to cybercrime in larger numbers than reported, due to being underprepared. Trotter et al. (2018) and Fawaz and Shin (2019) warned that with the increasing popularity of IoT devices in organizations, the majority of future cyberattacks will be initiated from personal devices and will target personal data and confidential information. Therefore, businesses ignoring the preparedness by not developing their understanding of threats will likely be the next victims of cyber adversaries.

Routine Checkups for Hardware and Software. Related to understanding threats, businesses conducting technology infrastructure assessment will likely be more secured, as they could discover risks, threats, and existing vulnerabilities before threat actors take advantage of those technical weaknesses (Bamakan & Dehghanimohammadabadi, 2015). In terms of software and personal digital devices, checking and updating software patches is considered a proactive defense, by getting ahead of cybercriminals attempting to exploit software vulnerabilities (Ge et al., 2018). Indeed, for SMBs with small budgets, patching is a short-term reinforcement for their IoT devices. While hardware attacks are not prominent, hardware are highly vulnerable to malicious microchip installation and reverse engineering attacks (Wagner, 2016). As a result, checking on hardware could expose and end an in-process physical cyberattack. Importantly, hardware provides the vital foundation for software; therefore, when hardware are compromised, all applications and network systems of an enterprise will presumably be exploited. The current

problem for cybersecurity in business is that, according to participants, SMBs do not perform routine checkups for hardware and software. Because of this, a few participants believed that they will be victimized in a near future. Given the importance of assessing the health of software and hardware, businesses building a proactive defense must routinely check their technology infrastructure to discover and eliminate vulnerabilities and to be aggressive in defending against cyberattacks.

Defense Capabilities. To be highly secured against cyber adversaries, SMBs are required to strengthen their defense capabilities. There are many measures for improving cyber defense that companies can apply to their infrastructures to avoid or mitigate cyberattacks. Nevertheless, the measures for improving cyber-defense capabilities are categorized into four competencies that cover all stages of a cyberattack. These four competencies address preparations before the attack to necessary action in the aftermath of a cyber breach. This section addresses defense capabilities in terms of how businesses prepare, prevent, detect, and respond to cyberattacks.

Prepare. Preparing for cyber defense is to prepare for cyberattacks. In respect to theoretical preparation, businesses need to develop foundational knowledge of the types and trends of cyberattacks in their specific industry and region (Bandler, 2018). Additionally, formulating an incident response plan and performing risk analysis based on digital security concepts of confidentiality, integrity, and availability is greatly recommended. Further, scenario-specific preparation and simulations would improve cyber resilience and responsiveness of businesses (Taitto et al., 2018). The fundamental approach is to deliver both threat-specific training and whole-systems exercise. Beyond human-centered preparedness, making cyber investments in upgrading and securing network infrastructure and software strengthens the immunity of most cyber breaches (Nagurney & Shukla, 2017). In fact, the less money invested in

cyber defense, the more financial damages occur to U.S. SMBs (Fielder et al., 2018). The point made by Fielder et al. (2018) is a dilemma for SMBs. SMBs often have limited budget. In addition, there are other issues such as leadership and lack of knowledge. Therefore, preparing for cyber defense is often neglected. Given these points, businesses must understand both internal and external environments to establish a concrete defense foundation.

Prevent. Assuming that all preparation steps are taken, it is crucial for businesses to prevent cyberattacks. In reality, the financial consequences of a cyber breach are severely higher than business spending on attack prevention (Brasington & Park, 2016). While cyber preparation focuses on strengthening the existing network infrastructure and cyber human resources, cyberattack prevention emphasizes making additional technology investments and implementing cutting-edge proactive mechanisms (Nagurney & Shukla, 2017). Specifically, these mechanisms are network infiltration prevention, multi-factor authentication technologies, and user-side encryption. Regarding the growing trend of prevention measures, more U.S. businesses are using artificial immunity-enhancing module for servers, as it ensures the availability of critical servers with inmate and adaptive immune functions (Tarao & Okamoto, 2017). This trend indicates that the future of attack prevention mechanisms includes artificial intelligence and machine learning technology (Okamoto & Tarao, 2018). Under these circumstances, making optimal investments for the latest proactive defense technology seems to be the foremost strategy for businesses to have the technical advantage in preventing future attacks. In fact, making optimal investments were discussed by participants as a solution for the limited resources. These optimal investments include choosing an affordable third-party, checking and updating vulnerable software, and implementing a cybersecurity culture with a focus on training and policy. Based on collected data, prevention steps focus more on human factors than technical elements.

Detect. Detection and prevention go hand in hand, as a detected threat is easier to prevent than an unknown one. The cyber capability of detection in a business is crucial to mitigate incoming threats, as it provides a clear operating picture and aids decisive action capabilities (Borum et al., 2015). For U.S. SMBs, a powerful combination of infiltration detection and prevention system is the ideal system to thwart most attacks, as it is comprised of one intrusion detection system agent, a load balancer device, and multiple intrusion response mechanisms (Korba et al., 2016). Additionally, according to Rai and Chukwuma (2019), an effective detection needs the implementation of a managed security service provider and security information event management, as they monitor the network 24/7. This recommendation comes from the belief that most cyberattacks occur over the network domain. Based on collected data, the current technical solution of SMBs is incapable of following Rai and Chukwuma's suggestion. Rai and Chukwuma and employees working for SMBs share the same suggestions for detecting threats. Therefore, interviewees encouraged the reliance on the third-party cybersecurity service. Importantly, cutting-edge technology and training programs alone cannot detect most malicious insider attacks (Clarke et al., 2019). Concluding from studying 42 U.S. SMBs, Clarke et al. (2019) stated that workplace satisfaction has an enormous effect on detecting malicious insider threats while also aiding cyber analysts in measuring the impact of a specific insider threat. With this point, an outstanding detection capability of a business requires not only the installation of cutting-edge technology but also the involvement of organizational management in improving workplace satisfaction to discover insider threats. In fact, this was the hope of many participants. The ideal detection capability requires the combination of both technology and organizational management.

Respond. Responding to threats and attacks depends greatly on steps taken and capabilities established in preparation, prevention, and detection (Rizov, 2018). According to the Cybersecurity and Infrastructure Security Agency (n.d.), cyber response is a collection of activities that businesses develop and implement to address detected cyber threats. The success of a cyber response is evaluated by the containment of the impact on organizational infrastructure. In a business environment, there are true positive and false positive threat alerts; therefore, the responding process must be capable of profiling security events and preprocessing detected data accurately (Lee et al., 2019). To enhance this responding, Lee et al. (2019) suggested the application of artificial neutral networks in business defense capabilities, which would greatly lower costs by reducing the involvement of security analysts and improve accuracy in addressing risks. In short, the framework of response emphasizes the triad of time, cost, and efficiency, which is tied to decision making and technology in an organization (Clay, 2015). With the increasing threat impact and frequency, Clay (2015) proposed the use of automated response to improve the triad of cyber-threat response through a unification process between organizational decisions and technological enhancement for building the defender's advantage. In short, response is a strategic step for which business cannot afford mistakes, as it decides the outcomes of threat impacts. In reality, based on collected data, SMBs do not have the capability to respond to cyberattacks. Hence, they often suffer the aftermaths.

Risk Management. The purpose of risk management in cybersecurity is to identify, evaluate, and prioritize all sources of risks, to minimize or eliminate the impacts of cyberattacks on businesses (Kure & Islam, 2019). By conducting risk management, businesses develop a better understanding of their cyber capabilities. This means that organizations can focus on the existing vulnerabilities and implementing appropriate measures to counter cyberattacks. More

importantly, risk management covers both technical and organizational elements of a companies. In reality, participants revealed that SMBs are highly inadequate in managing risks of cyberattacks. These circumstances are the result of many weaknesses existing in SMBs. To name a few, they are the lack of knowledge of leadership, numerous daily human errors, the absence of investment in the defense capability, and other elements outside of the SMBs' environment such as the advancement of technology. Below is the essence of risk management that no matter the size of a business organization, business decision-makers and IT professionals are highly suggested to adhere to for effectively manage cyber risks. This section discusses the identification of cyber risks and vulnerabilities and implementing strategic changes based on cyber risks.

Identify Risks and Vulnerabilities. Cyber threats in a business environment come from many sources that can overwhelm business management unless they perform risks and vulnerabilities assessments. Risk assessments must be conducted routinely because the business environment and technology advancement create rapidly changing circumstances (Hayes & Cappa, 2018). Importantly, network software, hardware, and strategic IT professionals are the priority in every assessment because they have the direct relationship and impact on the security posture of an enterprise. For risk analysis, organizational adaptations and attack interventions are the performance indicators (Scholz et al., 2020). While analyzing risks, with respect to the performance indicators, businesses should also address the fundamental changes in new technology, as the inability to adapt in a timely manner would make digital innovations a threat. In information security, confidentiality, integrity, and availability are the fundamental security objectives that all types of organization must achieve (Ioannidis et al., 2019). For businesses having confidentiality as the highest priority, utilization of common vulnerability scoring

systems and asset classification is highly recommended for risk assessment (Qassim et al., 2019). In contrast, for those valuing integrity and availability of the information systems, the industrial control system-specific vulnerability assessment is more applicable in providing the big picture of organizational vulnerabilities. With the methodology discussed, businesses must understand their security objective to rely on the appropriate methodology to reveal existing risks and discover incoming threats.

Implement Strategic Changes. Organizational changes including technological adoption have always been challenging to many businesses. For every strategic change, businesses often receive different responses from stakeholders such as resisting, championing, and accepting, for which leadership must mitigate any organizational resistance and encourage adaptation (Sonenshein, 2010). Contemporarily, U.S. SMBs are implementing more strategic changes in information systems and technology-related human resources, compared to large corporations (Sanders & Spiering, 2016). For implementing strategic changes effectively, including technology adoption to mitigate current and future cyber risks, middle managers play the most vital role because of their strategic involvement in bridging top management and ground-level employees (Ukil & Akkas, 2017). Importantly, their strategic involvement must include the top four cognitive and behavioral qualities which are championing alternatives, synthesizing information, facilitating adaptability, and implementing deliberate strategy. Additionally, Self et al. (2015) recommended the use of the balance scorecard as an assessment instrument for each component and stage of the change implementation. The major advantage of this assessment tool is that it includes all levels of the organization, which provides the crucial perspective of strategy alignment in terms of organizational context, past experiences, and future initiatives based on environmental scanning. In short, with communication and vision as the foundation, the safe

step-by-step approach for organizational changes in SMBs includes identifying the urgent needs, appraising the company's performance, multifaceted interactions, meeting at all levels for encouraging changes, implementing strategic changes with assessments, and repetition of vision-related messages ("Succeeding With Organizational Change," 2015). More importantly, all steps must fit under four frameworks: change drivers, organizational components, change process determinants, and outcome assessments (Král & Králová, 2016). In essence, the profound strategic changes including technology adoption with respect to cyber-risk management requires the crucial involvement of middle management, assessment instruments, the dependable step-by-step approach, and frameworks enabling the change.

Cyber-Defense Mechanisms. U.S. SMBs are suggested to rely on defense mechanisms to fight against cyberattacks. Business organizations with advanced defense mechanisms are less likely to be victimized by cyberattackers (Bach & Alshammari, 2013; Humayed et al., 2017; Reagin & Gentry, 2018). Technology-focused and human-centered are two attack approaches for cybercriminals to penetrate a defense network of a business organization (Shree et al., 2017; Trim & Lee, 2019). Therefore, cyber defense in U.S. SMBs should be designed to address technology-focused and human-centered attacks. After reviewing current literature, defense mechanisms are divided into four fundamental categories. They are technical defense, operational defense, managerial defense, and physical defense Weaknesses in any of these categories lead to major entry points enabling cyber criminals to take advantage of the cyber infrastructure. Unfortunately, data collection uncovered the shocking cyber circumstances of SMBs that the majority of SMBs do not have any of the four defense mechanisms. A few participants recommended some forms of remedies; however, the suggested remedies do not cover all four defense mechanisms. Below is the thorough discussion of components of cyber-

defense mechanisms. The below discussion attracted from multiple studies and research serves as the frameworks and goals for SMBs to plan and implement their defense capability.

Technical Defense. Technical defense refers to the use of software and hardware in computational devices and networks to defend against attacks with technological methods (Neal & Ilsever, 2016; Shree et al., 2017). Commonly, techniques associated with this defense classification are authentication, antivirus, firewalls, access control, and cryptography (Shree et al., 2017). Because of the advancement and frequency of cyber threats, the capability of technical defense is the game-changing factor for businesses, especially SMBs, as they are attacked more frequently (Fielder et al., 2016). As high-end security mechanisms are unaffordable to small and medium enterprises, Kaila (2018) recommended these budget-constrained companies to focus cyber investments on security for accounts, network systems, cloud computing, and confidential data. Although this recommendation cannot completely solve the dilemma between budget and security, Kaila believed that these strategic investments on specific technical defense mechanisms will secure businesses with the upcoming cyber threats.

Operational Defense. There are two approaches of operational defense, which are security policy and personnel training (Bach & Alshammari, 2013). There are two basic principles of security policy that a business must adhere to: its relation to technical defense and its compliance with governmental regulations (Srinivas et al., 2019). By having a comprehensive security policy tied to the technical infrastructure of an organization, employees are not only provided with strict guidelines but also improved with cyber-awareness ability (Kemper, 2019). In fact, practical in-place security policy influences behavioral change and sensitivity of employees that lead to safer human–computer interaction (Trim & Lee, 2019). Importantly, these policies must comply with governmental regulations because of multiple standardization

challenges in cybersecurity (Srinivas et al., 2019). Commonly, the framework authored by the National Institute of Standards and Technology is often applied in SMBs, due to its comprehensiveness and simplified process. Furthermore, business cannot implement security policy without personnel training. The process of personnel training starts from the top level of an organization and puts great emphasis on security policy and compliance plan (Kemper, 2019). To address the lack of enthusiasm of employees in training, the four best practices recommended by He et al. (2019) are relating training elements to employees' personal life, reinforcing procedures and security guidelines, promoting an organizational culture of awareness, and minimizing security fatigue for users. As discussed, the operational defense focuses exclusively on human elements of cyber-defense mechanisms while depending greatly on the technical defense.

Managerial Defense. Managerial defense relates to standards for hiring people and insider threats (Bach & Alshammari, 2013). Because skillful technology staffs are essential to an organization's cyber defense, hiring managers are obligated to recruit and retain qualified cyber professionals (Reagin & Gentry, 2018). Nevertheless, with 82% of businesses reporting an IT skill shortage, it is a challenge for U.S. SMBs to compete with larger corporations regarding hiring technology professionals (Petruzzelli & Sharma, 2019). To address that dilemma, Reagin and Gentry (2018) suggested partnership arrangements in which strategic components of infrastructure are outsourced to experts to minimize defense cost and possibly receive a higher level of expertise than hiring and developing cybersecurity staffs. Furthermore, insider threat is considered the emerging threat landscape to U.S. businesses (Er Amandeep, 2017). Under the lens of managerial defense, companies can limit threats posed from internal elements through three pillars, which are microsegmentation to identify "hot spots," cultural change to put the

organization in a preventive rather than reactive posture, and prediction to expose insider activities in a timely manner (Bailey et al., 2018). In addition, businesses are recommended to conduct analysis to monitor groups rather than a single employee and employ effective metrics such as employee attrition and workplace satisfaction. In the final analysis, managerial defense provides an interdependent support for operational defense, for which they secure the human elements of a business's defense capability.

Physical Defense. Physical defense refers to monitor and control systems that organizations utilize to neutralize physical threats to their technology infrastructure (Hu et al., 2016). Theoretically, a cutting-edge physical defense system must contain three components: communication, computation and control, and monitoring and manipulation (Humayed et al., 2017). Ideally, these components must possess the capability to address three threat sources, which are adversarial, accidental, and environmental. Contemporarily, due to the increasing cyber threats, cyber physical control systems are a trend in both business and cybersecurity fields, as computer-based algorithms are incorporated to broadly control and oversee possible threat elements (Tu et al., 2019). Despite the increasing adoption and automated benefits of cyber physical control systems, the biggest challenge for its deployment in U.S. SMBs is cost (Moeuf et al., 2018). Most small and medium businesses often have short-term strategies which prevents them from making long-term investments for strengthening physical defense via the adoption of cyber physical systems. Alternatively, Kure et al. (2018) recommended that businesses conduct a risk assessment on their physical defense with an integrated approach including threats, organizational elements, and stakeholders to discover security issues, identify vulnerabilities, and analyze threat levels. By doing so, businesses would acknowledge the weaknesses of physical defense to strengthen them with other means to compensate for the

ability of cyber physical systems that are too expensive for SMBs to adopt. Moeuf et al. (2018) predicted that cyber physical systems will be more affordable, as costs of their components such as sensors are decreasing, which means that these systems will be widely adopted by SMBs. As shown, although physical defense is an important component of cyber-defense capability, cost is the dominant roadblock that prevents U.S. SMBs from implementing the latest physical defense technology.

Disaster Recovery and Business Continuity. Impacts of cyberattacks are inevitable due to both technology advancement and organizational weaknesses. Therefore, it is vital for businesses to recover and maintain their operation in the aftermath of an attack. In fact, disaster recovery and business continuity are more vital for U.S. SMBs than large enterprises and multi-national corporations (Herbane, 2019). Due to organizational size, SMBs would suffer from greater losses from cyberattacks than larger enterprises. As a result, disaster recovery and business continuity are the strategic capabilities that SMBs must obtain to persist through consequences of a cyber catastrophe. This section focuses on disaster recovery and business continuity in SMBs.

Disaster Recovery. The ability to recover quickly in the aftermath of a cyberattack depends greatly on threat intelligence gathered from components of the risk assessment process (Tounsi & Rais, 2018). For all sizes of businesses, a disaster recovery plan must include all departments and both internal and external environments (Kachgal, 2015). Importantly, crisis communication plans and emergency response procedures must be addressed in the plan with the objective of business resiliency. The smaller the size of a business, the more impact it has from uncertainties and risks (Herbane, 2019). Therefore, SMBs must include more details addressing further threats than corporations. In short, impact analysis and risk assessment, emergency

response and crisis management, communication procedures, and frequently auditing and exercising disaster recovery plans are the essence to strengthen organizational resilience of SMBs (Sarmiento et al., 2016). Given these points, compared to larger organizations, disaster recovery plays a greater role in SMBs, as they do not possess the size capable of withstanding severe disaster.

Business Continuity. It is estimated that 25% of SMBs do not reopen after a major disaster (Sarmiento et al., 2016). An effective business continuity plan must consist of two parts: value preservation and value creation (Niemimaa et al., 2019). More importantly, to ensure these two values during and after the disaster, decision makers must incorporate their organization' business model and stakeholders. In application, the steps to do so are defining the business model, identifying uncertainties, accessing impacts, and designing changes. Regarding cyberattacks in business, the plan for continuity must address common cyber threats, importantly, the impact of data breaches (Phillips & Tanner, 2019). Notably, the main weaknesses of continuity plans in businesses are the lack of cybersecurity culture, management support, and effective responses. These weaknesses were the central points discussed by participants as the organizational challenges. As a final point, the reviewed literature on business continuity and collected data show that U.S. businesses do not have the adequate plans to ensure their operation during and after a disaster. This reality weakens the capability of cyber defense, as business activities are severely disrupted as an aftermath of a cyberattack.

Weaknesses of Cyber Defense. SMBs are highly vulnerable because of various weaknesses in their cyber defense. These weaknesses include both human factors and technical elements. By exploring current weaknesses in cyber defense, decision makers in businesses would be informed to implement strategic changes in their organizations to improve cyber

defense. Contemporarily, ineffective security awareness training, lack of security skills, and negligence in safeguarding critical information are identified as weaknesses in organizations (Cain et al., 2018; Dominitz, 2017; German, 2018; McCormac et al., 2017). This section focuses closely on the three identified weaknesses.

Ineffective Security Awareness Training. In dealing with cyberattacks, U.S. SMBs have and continue to invest in technology-based solutions (Abawajy, 2014). This approach exposes them to social engineering attacks, as organizational resources are diverted away from security awareness training programs. Fewer than 33% of surveyed employees rated their security training as effective (Caldwell, 2016). As a result, data breach is the biggest concern generated from the ineffective security awareness training (Kennedy, 2016). Specifically, behavior and attitudes of employees, incompetent security information, and the lack of practices results in worthless training programs in businesses. Additionally, training alone cannot achieve organizational objectives for cyber defense when cybersecurity culture is not incorporated and preserve (Hanus & Wu, 2016). As reviewed, ineffective security awareness training is a threat to the whole cyber-defense capability of businesses.

Lack of Security Skills. One of the eminent cyber-threat landscapes for U.S. SMBs is skill shortage, due to the advancement of technology, the increase in cyberattacks, and better talent attraction in corporations (Petruzzelli & Sharma, 2019; Smith, 2018). Currently, 70% of surveyed working cyber professionals report that the lack of cybersecurity workers is severely impacting their workplaces (Smith, 2018). Adding to this weakness, while the demand for cybersecurity graduates is beyond the abilities of universities to produce, their lack of real-world security experience remains a problem for companies (Basken, 2017). To summarize the problem of security skills, Cameron and Marcum (2019) reported that in 2018, 51% of U.S.

businesses reported that they have a shortage problem, while the figure was 28% in 2014. Also, the concern of companies regarding the ill-prepared newly graduated cyber workers rose by 6% per year. With this trend, the lack of security skills will soon be a crisis that weakens the cyber defense of many companies, especially SMBs, as they are disadvantageous in competing with corporations with respect to talent attraction.

Negligence in Safeguarding Critical Infrastructure. Negligence of technology workers is the most common key to a successful cyberattack (Hayden, 2015). Specifically, web-based attacks and information breaches are typically the consequences of negligence (Safa et al., 2015). Safa et al. (2018) indicated that negligence of cyber professionals is often a result of new involvement with specific security activities, the lack of attention to environmental factors, and rationalization of a misbehavior. While many argue that awareness training would reduce breaches caused by negligence, Chen et al. (2015) stated that training alone is not effective at all. They believed that a comprehensive security program with a series of strict guidelines and regulations would impact and modify employees' behaviors toward cybersecurity, which reduces negligence. In fact, after researching the application of this solution in businesses, Chen et al. (2015) concluded that their suggested security program did change cyber professionals' behaviors and facilitate deeper thoughts on cyber defense value and beliefs. Nevertheless, it will be long before comprehensive security program becomes a solution for U.S. SMBs to combat negligence because, as revealed, they believe the policy-based approach has low return-on-investment value (Almeida et al., 2018).

Theories and Principles of Cyber Defense

With the growing need for incorporating cybersecurity in businesses, conceptual frameworks addressing these fields are highly valuable in guiding business decision makers in

implementing the appropriate cyber defense based on their organizational structure. Serving as the conceptual connection between technology and enterprises, selected conceptual frameworks must be relevant to business practice and real-world circumstances. Based on data collection, cyber situational awareness theory, cyber defense mechanisms theory, and Control Objectives for Information and Related Technology (COBIT) 5 are considered relevant to the circumstances of cybersecurity in SMBs. These three conceptual frameworks provide companies, especially small and medium ones, the application framework to develop and improve their cyber-defense capabilities while complying with their business process. Particularly in respect to cyber defense, cyber situational awareness theory focuses on human resources to strengthen the organizational side of security, cyber defense mechanisms theory discusses the technology implementation with advantages and disadvantages of a different approach and risk-based strategy, and COBIT 5 covers how businesses incorporate cybersecurity into their organization with the optimal security outcome, highest return on investments, and the least organizational resistance.

Cyber Situational Awareness Theory. Obtaining cyber situational awareness is considered gaining a strategic advantage over adversaries (Lenders et al., 2015). With better cyber situational awareness, companies can greatly decrease the probability of being a cyber victim (Kemper, 2019). The application of cyber situational awareness theory contributes greatly to the decision-making process of business leaders and stakeholders involved with an organization's defense system (Franke & Brynielsson, 2014). Elements of this theory may be analyzed in terms of business environment and cybersecurity. This section discusses the current state of situational awareness in businesses, network situational awareness, threat situational awareness, mission situational awareness, and the application of cyber situational awareness theory to companies.

Situational Awareness Is the Weakest Link in Businesses. Because 90% of cyber breaches result from human error, situational awareness of employees in businesses is the weakest link of cyber-defense capability (Kemper, 2019). Specifically, situational awareness is the forefront for companies in the fight against cybercrime because it involves the acknowledgement of how the network is operating and what information and activities of stakeholders (i.e., staffs, business partners) are influencing the information systems (Chen et al., 2016). Chen et al. (2016) and He and Zhang (2019) reported that many IT professionals ignore abnormal network activities and fail to act on system alerts. Because awareness is a human capability, it requires a lengthy progress to change employees' cyber-insecure behaviors and build an organizational culture of cyber awareness (He & Zhang, 2019). Furthermore, many cyber professionals reported that situational awareness is a highly specialized skill, one which human resources in a business environment lack (Dawson & Thomson, 2018). Additionally, it is challenging for businesses to improve awareness skills through hiring, as there is a shortage in the cyber workforce and new graduates do not have the adequate cognitive task analysis that may be gained from work experience. Assessing cyber situational awareness of SMBs based on the threat landscape, Newmeyer (2015) concluded that there is an enormous gap between human resources' analysis ability and the advancement of cyber threats, especially with the growth of IoT devices. This infers that, while sources and complexity of threats are expanding, cyber situational awareness of employees in business is severely inadequate in facing new challenges. Therefore, cyber situational awareness will remain the weakest link in the cyber-defense capability in the long term.

Network Situational Awareness. The network is a critical domain serving as the medium for technical communication in businesses. Therefore, any abnormal activity indicated by

security parameters of the network must be acknowledged and responded to by employees to detect possible intrusion attempts (Rapuzzi & Repetto, 2018). From the intrinsically cognitive dimension regarding network users, there are three levels for network situational awareness that must be followed through to respond quickly and effectively to a possible risk (Erbacher et al., 2010). Friedberg et al. (2015) argued that human responses and decisions are currently the problem for the low-level network awareness in many businesses, as employees are provided with network anomaly detection tools such as network partitioning and software or hardware appliances. Believing that IoT and cloud computing are the emerging challenges for network security awareness, Azhagiri et al. (2017) proposed that the model of multi-level detection analysis, which currently has limited implementation in SMBs, must be incorporated in organizations to effectively expose stealthy attacks and proactively alert responsible IT workers. This model focuses on the technology side of network awareness, which involves six detection subsystems working independently and interconnectedly: malware detection, intrusion detection system and firewall, vulnerability scan, penetration testing, online testing, and security service detection. As a review of the literature addressing network awareness revealed, this type of awareness emphasizes both human involvement and functions of technology.

Threat Situational Awareness. Threat situational awareness addresses the ability of stakeholders in information systems to process the finding of true threat signals among the existing massive amounts of collected data (Alnusair et al., 2017). In short, it is a threat assessment methodology based on a certain cyber situation. This methodology includes the prediction of the upcoming threat and attack path, identification of countermeasures, and planning countermeasures based on organizational policy and technology (Park et al., 2019). Importantly, unlike network awareness, threat situational awareness covers both technology-

based attacks and human-centered attacks. Homoliak et al. (2019) believed that threat situation awareness should be prioritized in training programs and human resource development as it provides the fundamental support for reducing insider threat and social engineering risks especially at application level and business process level. Furthermore, regarding the massive growth in adoption of IoT devices in small and medium businesses, enhancing threat intelligence situational awareness is improving human-data interaction in which cognitive process of employees purposefully filter multi-media data sources (Alnusair et al., 2017). Information impacting enterprise network occurs in real time; therefore, strengthening threat situational awareness will provide employees with fast and effective solutions when exposed to a risk from IoT (Riesco & Villagra, 2019). With the broad scope that covers both technology-based attacks and human-centered attacks, it seems that acquiring the high-level threat situational awareness is the strategic implement for SMBs in tackling challenges from the threat landscape.

Mission Situational Awareness. Mission situational awareness is the ability to identify both possible hazards and threat types that are associated with the system architecture and mission objectives (Bakirtzis et al., 2017). During the execution of a business plan or strategy, awareness sinks to critically low as stakeholders often focus exclusively on particular tasks (Lukosch et al., 2015). Therefore, maintaining situational awareness in respect to the ongoing mission is significantly crucial to safeguard the outcomes of the planned mission. To do so, in a business environment, Lenders et al. (2015) suggested the following of an OODA (observe, orient, decide, act) loop, with the narrow scope and boundary on the cyber domain. Additionally, mission-related information, especially with regard to information output and input, should be shared sequentially among business team members to develop their own awareness (Lukosch et al., 2015). In short, all stakeholders involved in a mission can maximize awareness through

preparing for the continuous assessment of threat environment, anomalous activity, vulnerabilities, key terrain, operational readiness, and ongoing operations (Dressler et al., 2014). In essence, to be highly aware of threats targeting a business mission, stakeholders are responsible for preparing in a manner so that their mission elements will endure a malicious attack and achieve planned business objectives.

Incorporating Cyber Situational Awareness Theory. Given the strategic advantage of having a high-level awareness in businesses, business decision makers are highly recommended to incorporate cyber situational awareness to their human resources and technical infrastructure (Lenders et al., 2015). With this purpose, awareness training programs are the most practical at all levels of an organization. Besides the current training approach in businesses, Miranda (2018) recommended exercises on various realistic scenarios and feasible responses with scripted procedures. Additionally, training for each threat should have its own design, methodology, and intervention. As U.S. business spending on training programs grew to $70 billion in 2015, SMBs can reduce training costs while maximizing return-on-investment by utilizing learning management systems (Korpela, 2015). Specifically, the financial leverage of employing learning management systems in low-budget companies is to improve awareness training with a personalized learning experience, increase end users' attendance and compliance, and reduce management's involvement. Furthermore, intensive situational awareness performance tests must be conducted routinely to assess the possibility of human error for each error category (Marquardt, 2019). While error categories are varied on the basis of organizational structure and network architecture, most common are lack of knowledge, lack of awareness, distraction, and social norms. After all, the utmost objective of incorporating cyber situational awareness theory is to construct and maintain a business culture that has fully aware employees on their

organizations' cyber frontline defending against cyberattacks (Rahim et al., 2015). Only when this utmost objective is achieved, cyber breach will rarely occur.

Cyber Defense Mechanisms Theory. The cyber defense mechanisms theory focuses on the principle of denial-of-attacks (Ryan, 2018). The principle of denial-of-attacks argues that if the defense capability of an organization is powerful, adversaries will not attack because of the negative cost/benefit ratio. In other words, cybercriminals are discouraged to attack companies with a strong cyber defense because the cost of time and effort is greater than the benefit. The principle of denial-of-attacks has proved its effectiveness as a national defense strategy (Lee, 2015). Therefore, this principle is highly applicable to the fields of cybersecurity and business. To examine the cyber defense mechanisms theory, denial-of-attacks strategy, passive defense mechanisms, and proactive mechanisms are critically examined in circumstances of SMBs.

Denial-of-Attacks Strategy. Threat actors cannot compromise an information system when that system is highly secured. Theoretically, denial-of-attacks strategy discourages attackers' motivation to conduct cyberattacks by denying them the means to compromise (Ryan, 2018). Because method and time of an attack are unexpectable, businesses following this strategy are required to develop innovative defense technologies with dynamic, heterogeneity, and redundancy mechanisms (Hu et al., 2018). Notably, technologies alone cannot defeat malicious intention of threat actors. As only 9% of SMBs has information security as their organizational culture, they are greatly vulnerable to human-centered attack types (Kaušpadienė et al., 2019). In fact, ignoring human involvement in a system, SMBs are creating a different problem, but no less challenging as cyber-defense mechanisms incorporate both technology and human resources in organizations (Mulligan & Schneider, 2011). Although not focusing exclusively on human involvement as in cyber situational awareness theory, denial-of-attacks

strategy still relies on organizational elements for its two common mechanisms and approaches: proactive and passive (Ryan, 2018).

Passive Mechanisms and Approach. The majority of current defense mechanisms in SMBs are passive mechanisms (Amao, 2015). Passive mechanisms are the foundation of cyber defense in network systems, as they fulfill security gaps by protecting against threats without regular involvement of human analysis (Cho & Ben-Asher, 2018). The primary approaches of passive mechanism are reconnaissance defense, intrusion detection, and intrusion prevention, with the interdependent connectedness of hardware and software such as firewalls, anti-malware systems, and cyber physical control systems. With the outgrowth of cyberattacks recently, deception is believed to be an approach of passive defense despite some cyber experts arguing that it falls under the category of proactive mechanisms (Gartzke & Lindsay, 2015). In practice, deception defense mechanisms employing by organizations are highly impressive in delaying the intruder's exploitation of confidential data by burdening them with false leads and sorting costs. Importantly, Gartzke and Lindsay (2015) reported based on experiments that a deception approach could even harm the attacker's technical resources. Nevertheless, despite passive mechanisms' popular usage in U.S. enterprises, the advancement of technology and the growing number of threat actors have driven these mechanisms to become outdated and incapable of defeating well-planned and complex attacks (Jajodia et al., 2016). Therefore, the most secured approach to cyber-defense mechanisms is to implement both proactive and passive measures working interrelatedly.

Proactive Mechanisms and Approach. Similar to military doctrine, an effective cyber-defense system is one that can deter aggression with aggressive intimidation and coercive responses (Davis, 2014). As a result, proactive defense becomes a new norm in the cybersecurity

field, with the active approach of gathering intelligence to prevent future attacks and predicting when and how the cyber strike occurs based on realistic evidence (Lonsdale, 2018). Specifically, a proactive cyber-defense system in a business would follow a four-phrase cycle: threat intelligence consumption, asset identification and network security monitoring, incident response, and threat and environment manipulation (Lee, 2015). The purpose of the four-phase cycle of proactive defense is to actively monitor for, respond to, and learn from threat actors. This methodology is supported by advanced technological measures and tactics such as white worms, honeypot deployments, honey net, spam traps, sandboxing, and penetration testing (Dewar, 2014). Given the active engagement in defending against threat actors, proactive mechanisms and approach is the strategic deployment for U.S. SMBs in reducing cyberattacks.

Comparisons of Passive and Proactive Approaches. While both proactive and passive mechanisms and approaches must be utilized in businesses to counter all sources of cyber threats, each type has its own advantages and disadvantages. While proactive defense has an enormous potential for limiting the number of threat actors and risks from emerging technology, some practices of the proactive approach may prove to be illegal, due to regulations stated in the U.S. Computer Fraud and Abuse Act (Dewar, 2014). Specifically, “hack-backs” fall on the thin blurry line between unauthorized access and tracing attackers’ technological architecture (Dewar, 2014, p. 10). On the other hand, having merely passive mechanisms makes organizations considerably vulnerable, as the number of cyber breaches is rising sharply, especially the massive loss of information assets in companies (Neal & Ilsever, 2016). Therefore, Neal and Ilsever (2016) reported that 36% of surveyed organizations have begun to conduct cyber active defense. Importantly, incorporating proactive mechanisms to boost the cyber-defense capability of a business is not as easy as installing software and hardware as in passive

mechanisms. Costs, human resources, and expert skills are the biggest dilemma for organizations, especially SMBs with low budgets (Slayton, 2017). With 82% of organizations reporting a cyber-skill shortage (Petruzzelli & Sharma, 2019), personnel factors are seen as the second highest expense for fully implementing proactive defense mechanisms (Slayton, 2017). Given the disadvantages and advantages of both passive and proactive defense mechanisms, Denning and Strawser (2014) believed that, while recommending implementing both approaches, the option is open to private entities in respect to how far they are willing to strengthen their network infrastructure.

Application of Cyber Defense Mechanisms Theory in Business. As discussed, it is vital to implement both passive and proactive cyber-defense mechanisms. Concerning this point, Hadji-Janev and Bogdanoski (2017) suggested the use of swarming-based cyber defense built under the framework of collective security which, although the recommendation is geared toward national defense, SMBs can rely on to confront threats by overwhelming their sources. This recommended framework requires the interconnectivity and interdependence of technical hardware and software which, additionally, helps organizations to meet the changing security landscape. Equally important, incorporating social and behavioral elements in defense gives vulnerable businesses the advantages of human-centered countermeasures through human resources training, organizational development, and situational awareness improvement (Granåsen & Andersson, 2016). Besides the proposed approach in passive and proactive mechanisms, cyber insurance is a fast-growing trend for SMBs (Xu et al., 2019). Although cyber insurance is not directly related to the conventional methodology (technical mechanisms and human-centered countermeasures) of cyber defense mechanisms theory, this rising trend supports the defense capability by transferring risks, reducing financial loss, and, based on

specific liability policy, adding third-party security layers (Bodin et al., 2018; Wang, 2019; Xu et al., 2019). As shown above, incorporating cyber-defense mechanisms in organizations requires well-planned strategies and careful considerations in terms of choosing appropriate technical measures and implementing human resources development. Therefore, businesses need to be prepared for organizational changes (Lee et al., 2015).

Control Objectives for Information and Related Technology (COBIT) 5. COBIT 5 is considered to be the most integrated and comprehensive framework for SMBs to apply to their technology infrastructure (Rubino et al., 2017). COBIT 5 is highly integrated and comprehensive because this theory covers most aspects of both business environment and cybersecurity. In reality, security and functionality of technology in businesses have been greatly enhanced through the application of COBIT 5 (ISACA, 2012a). As COBIT 5 has proven its effectiveness in business world, it is important to explore components of COBIT 5. This section examines and discusses seven core principles of COBIT 5 that elevate businesses to better levels in cybersecurity and business operation.

Application of COBIT 5. Although COBIT 5 does not focus exclusively on cyber defense, it is considered the most comprehensive and applicable framework for businesses to transform the overall cybersecurity capabilities while accounting for organizational changes and resistance to change, in terms of implementing new security technology and business process and operation (ISACA, 2013). Additionally, this framework sets the clear guidelines and direction for decision makers to discover their cyber vulnerabilities through intensive risk management and all facets of business technology such as operations, installations, legal compliance, and audit. Specifically, COBIT 5 emphasizes IT governance, which covers five extents, which are governance, compliance, IT operations, security and risk management, and IT audit and

governance (Alkhaldi et al., 2017). By applying COBIT 5, businesses would achieve up to 40% higher return on technology investments than those who do not (Devos & van de Ginste, 2015). Because this framework covers numerous technology resources and human elements of an enterprise, it is recommended that businesses should pick the most appropriate application based on the fit between the framework and organizational interest, the context of the organization and COBIT 5 standards, future impacts after implementation, and managerial contribution (Anomah & Aduamoah, 2018; Devos & van de Ginste, 2015). Furthermore, with respect to cyber-defense capability, two focuses of COBIT 5, IT processes and risk management, could provide decision makers better perspectives on making strategic decisions such as managing IT problems, network and technology services for stakeholders, and identification and assessment of threats (Nicho, 2018). In fact, in the domain of deliver, service, and support, Jarsa and Christianto (2018) reported that businesses with IT vulnerabilities applying COBIT 5 framework have improvement from an average capability level to level-one performed process. Unsurprisingly, this achievement made possible by COBIT 5 is the result of its functional aspects and social aspects. Functional aspects consider the structural and process requirements in organizational design elements, while social aspects cover stakeholder behavior and company culture (Amali et al., 2020). In essence, the functional and social aspects of COBIT 5 are the objectives of its five principles that have successfully elevated countless companies to higher levels of security and functionality (ISACA, 2012a). These five principles are meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, and enabling a holistic approach. By incorporating these fundamentals, it is foreseeable that U.S. SMBs will be more secured through having a concrete IT infrastructure and well-informed human resources.

Principle 1: Meeting Stakeholder Needs. Different stakeholders in an organization have their own needs and expectations. The principle of meeting stakeholder needs supports the recognition of each type of stakeholder, with negotiation and decision-making processes across various needs (Boonstra et al., 2018). Specifically, contrasting and shared interests, values, and beliefs of stakeholders shape the application of this theory in a business environment. The underlying purpose is to align these needs with IT goals and, more importantly, organizational objectives (Vincent, 2016). Baillette and Barlette (2018) noted that organizational change in terms of technology implementation for SMBs requires the consideration of employees' needs as, due to the organization size, business decision makers and employees have a more direct relationship than in larger corporations. Therefore, this principle plays a significant role for both entrepreneur–employee relationship and deploying new technology in U.S. small and medium enterprises.

Principle 2: Covering the Enterprise End-to-End. This principle indicates the governance approach of governance enablers and governance scope, which concentrates on three objectives: benefit realization, risk optimization, and resource optimization (ISACA, 2012a). Specifically, governance enablers address management framework, organizational policies, and IT project structures (Jugdev, 2019). In short, the strongest enabler in a business organization, according to Jugdev (2019), is discursive ability. Furthermore, governance scope relates to roles, activities, and relationships within the scope of management activities and domain that will be influenced by governance systems (Hammer, 2013). In brief, this principle covers all organizational elements and management practices and sets the scope and boundary for the betterment of management of information systems and other technology assets.

Principle 3: Applying a Single Integrated Framework. The structure and nature of COBIT 5 is a single integrated framework. The single integrated framework means it aligns with other latest standards and frameworks, covers an enterprise fully, provides a simplified IT architecture for formulating guidance, and integrates all previous frameworks of the ISACA organization (Behnsen & Faber, 2012). By applying a single integrated framework, organizations will spend less time and effort searching for and using multiple conceptual foundations. It will be less confusing for business management to rely on a single comprehensive framework. In fact, the single integrated framework is the result of continual changes in business process and information systems influenced by customers and suppliers and, importantly, pressured by cybersecurity regulation.

Principle 4: Enabling a Holistic Approach. This principle is applied once cyber-defense mechanisms and governance programs are in place (Behnsen & Faber, 2012). Specifically, the holistic approach covers seven interacting enablers, which are (a) principles, policies, and frameworks; (b) processes; (c) organizational structures; (d) culture, ethics, and behavior; (e) information; (f) services, infrastructure, and applications; and (g) people, skills, and competencies (ISACA, 2012b). In other words, these enablers are the factors directly influencing the outcomes of IT project management and the implementation of the new business process. Importantly, the vehicles supporting these enablers are principles, policies, and frameworks, which translate management guidance to daily management. Regarding SMBs, by having the holistic approach from applying this principle, internal audit would have a full range of IT risks and risk management challenges (Vincent, 2016). Relating to cyber-defense capability, this principle supports the selection of cyber-defense mechanisms, as decisions makers are provided the tools for cyber-risk management (van Wyk & Rudman, 2019).

Principle 5: Separating Governance from Management. The distinction between governance and management in an organization must be clearly defined and distinguished to differentiate specific roles and responsibility (ISACA, 2012b). Governance is the structure and process that evaluates and monitors IT mechanisms (Setiawan & Andry, 2019). Governance ensures that objectives are achieved through prioritizing decisions and complying with stakeholders' needs based on the organization's capability. On the other hand, management, as defined in COBIT, is the combination of plan, build, execute, and control, with the purpose of ensuring that all business activities are aligned with the direction and guidelines of governance (Rubino et al., 2017). Regarding governance and management in COBIT 5, this conceptual framework recommends 37 IT processes for which business organizations, based on their evaluation of size, capability, and complexity, can rearrange their business processes as decision makers see fit (ISACA, 2012a).

Summary of the Literature Review

This section examined three strategic areas of cyber defense in U.S. SMBs. Based on the thorough overview of existing literature addressing cybersecurity in SMBs, the first part of the literature review discussed the impacts, approach, and future trends of cyberattacks against SMBs. Specifically, organizations will not only suffer financial loss as an aftermath of each attack but also damages to intangible assets and customer trust. More importantly, there are many common sophisticated attacks with both technology-based and human-centered methods threatening SMBs. Also, as reviewed, the future of the threat landscape is unfavorable to the private sector due to advancements in technology and organizational unpreparedness. Next, the cyber defense section addressed the defense capability of businesses to defend against cyberattacks. In particular, this section identified and explored components of cybersecurity that

SMBs could implement and strengthen in order to safeguard their organizations. In short, the essence of an effective defense requires the improvement of defense technology, enhancement of human resources, and implementation of organizational strategies. Along with the cyberattack and cyber defense sections, the final section of the literature review related to conceptual frameworks and concentrated on the conceptual application that SMBs could use in their organizations to develop stronger defense capability. These frameworks cover both technology-based and human-centered approaches to support businesses fighting against all methods of cyberattacks.

Transition and Summary of Section 1

In this foundation of the study section, background information was provided to highlight numerous business issues and cybersecurity elements of the growing number of cyberattacks critically threatening U.S. small and medium enterprises. The background of the problem, problem statement, purpose statement, and research questions were explored and structured based on the concern of escalating cyberattacks against U.S. private entities. More importantly, the nature of the study and conceptual framework were strategically selected to support the researcher in guiding the process of this research. Likewise, the significance of the study emphasized the importance and benefits of conducting this research with respect to the reduction of gaps, implications for biblical integration, and relationship to the field of study. Next, assumptions, limitations, and delimitations were determined and discussed to set the clear scope and boundary. The comprehensive literature review addressing cyberattacks, cyber defense, and conceptual framework provided an overview of the current circumstances and conditions related to cybersecurity and organizational elements in U.S. small and medium companies. The next section, section 2, will discuss multiple components of the gathered data. There will be a

discussion of data types and collection methods. Equally important, the data analysis methods in conjunction with a resulting summary of the results will be included.

Section 2: The Project

This section discusses thoroughly the qualitative method with a case study design approach that was used in this study. This section begins with a purpose statement to help readers clearly understand the intent and focus of the study on the ongoing problem of U.S. businesses continuing to fall victim to cyberattacks. In addition, the role of the researcher will be discussed regarding tasks of designing the research, collecting and maintaining acquired data, and conducting data analysis. Furthermore, following the role of the researcher's section, procedures for gaining access to participants, establishing a relationship with participants, and setting measures to ethically protect participants will be closely examined. To provide a strong foundation for this study, the research method and design section will provide a detailed discussion for each study method and design. This section will also identify the selected research method and design and address reasons for the selection regarding the problem of cyberattacks in U.S. business and the purpose of the study. Next, the population and sampling section will address population size, sampling size and method, sampling frame, eligibility criteria, and relevant characteristics of participants. The data collection section with three parts, the instrument of the study, data collection technique, and data organization, will define and standardize all components of the data collection process based on the purpose and problem statement. Based on the components of the data collection section, the data analysis section will provide a detailed discussion of the coding processes, which were used to identify relevant themes and perceptions of the problem of cybersecurity in U.S. businesses. Finally, the qualitative reliability and validity will be demarcated thoroughly throughout this study.

Purpose Statement

The purpose of this qualitative research was to reveal the contemporary barriers and challenges that impact the latest cybersecurity competencies of small and medium enterprises, through a study of the perception and experience of these organizations regarding cyber defense as a business risk. This study explored the increase of cyberattacks based on technical factors and organizational elements, considering that the effectiveness of cybersecurity requires both technology and business strategies (James, 2018). The research focused specifically on small and medium businesses in the U.S. private sector with fewer than 250 employees. The main objective was to identify the impacts of technical barriers, business strategy, and organizational elements causing cyber vulnerabilities that may result in small and medium businesses becoming cyber victims. Therefore, the cyber-defense capabilities of SMBs were the primary focus of this study. Because existing studies approach the issues of cyberattacks in the business field with either technology-assisted attacks or technology-focused attacks (Donalds & Osei-Bryson, 2019), this study fulfills the gap in both cybersecurity and business fields by adding the human factor and organizational effectiveness elements to the existing body of knowledge. The end goal was to provide SMBs with breakthrough information that could initiate changes in their organizations to defend against the ever-increasing number of cyberattacks in the business sector.

Role of the Researcher

In all studies, the researcher involves him or herself with the research process from the beginning to the final stage of the study. No individual is more important than the researcher conducting the study. Therefore, it is critical for all researchers to identify their roles and responsibilities in studies. With that being said, the role of the researcher in this study will be thoroughly discussed to ensure that all research tasks were completed and goals were well

fulfilled. More succinctly, the role of the researcher is designing the research, collecting and maintaining acquired data, and conducting data analysis.

Designing the Research

The researcher must precisely conduct the designing of the research study to create a well-built foundation for the research. This process consists of formulating, planning, categorizing, and implementing consequential steps and procedures that adhere to the course of the research (Stake, 2010). In short, the role of the researcher in designing the qualitative research must ensure four crucial qualities: credibility, dependability, confirmability, and transferability (Whittemore & Melkus, 2008). Furthermore, as Stake (2010) suggested, based on the purpose of the study, the researcher's role was to determine which technique of data collection was the most appropriate. With a case study as the research design, interviews are a suitable and useful data collection technique to achieve the desired outcomes of many qualitative studies (Creswell & Poth, 2018; Whittemore & Melkus, 2008). When a data collection technique is selected, the role of the researcher is to develop qualification criteria for participants and decide whether data should be collected from individuals or groups (Magnusson & Marecek, 2015). Next, designing the research also involves choosing the most suitable method of conducting the data collection. As case study was the research design of this study and semi-structured interview was chosen as the data collection technique, the method of conducting data collection included face-to-face, telephone, and video call. The last task of designing the research is to define how much data should be collected.

Collecting and Maintaining Acquired Data

The process of collecting and maintaining acquired data in a qualitative research study requires a greater involvement of the researcher than in quantitative research, as the qualitative

researcher directly serves as the fundamental data collection instrument (Creswell & Creswell, 2017). With semi-structured interview as the data collection technique, the researcher chose participants based on qualification criteria, recorded participants' interviews, checked and transcribed interviews, and captured noteworthy details and context occurring during participant interviews. During the interview process, contextual clues such as participants' reactions, behaviors, and nonverbal signals are crucial for building strong research (Sutton & Austin, 2015). It is important to note that a significant amount of data is often acquired in qualitative research (Creswell & Poth, 2018); therefore, the researcher cannot make any errors in maintaining the acquired data. To properly safeguard and preserve the integrity of acquired data, the researcher created and followed a strict system of collecting, storing, and organizing data throughout the research process (Demchenko et al., 2012). By doing so, the researcher achieved the desired outcomes of the study.

Conducting Data Analysis

Conducting data analysis is the rational way to recognize the meaning of data acquired from study participants (Chenail, 2012a). Data analysis consists of inspecting, cleansing, interpreting, and selecting data based on the goals of the research. Chenail (2012b) indicated that one of the biggest challenges of data analysis in qualitative research is to decide what piece of data "constitutes a meaningful unit to analyze" (p. 266). To tackle this challenge, the researcher, based on recommendations of Sutton and Austin (2015), developed a coding process and relied on this process to relate and connect acquired data from participants. The next step was to identify common themes across interview transcripts. Once data saturation was reached, the researcher verified, synthesized, and presented the findings by generating a well-detailed report.

To ensure precise findings with true meaning, the researcher will support the report with references to study participants' actual quotations.

Participants

This research could not achieve its purpose without the involvement of participants. Only participants can accurately portray the contemporary picture of the problem of cyberattacks in U.S. businesses. Because participants were cyber professionals currently working in U.S. SMBs, the researcher carefully developed a well-planned procedure to approach and invite them to participate in the study. In addition, the researcher took into consideration the sensitivity of the occupations of participants and the confidentiality of the cybersecurity field. In detail, the procedure consisted of gaining access to participants, establishing a relationship with participants, and taking measures to ethically protect participants.

Gaining Access to Participants

Gaining access to participants is the most fundamental task of fieldwork for a qualitative research study. As a member of multiple cybersecurity groups and forums across the United States, the researcher had access to a list of cyber professionals working in U.S. SMBs, who could offer insights into current cybersecurity issues and trends. More importantly, they were currently employed by multiple U.S. businesses. Initially, the researcher extricated the list of cyber professionals, based on the delimitations proposed in this research, to create a list of research candidates. Once the list of qualified cyber professionals to interview was narrowed down, the researcher initiated contact via telephone, video calls, and social media messaging services to invite them to participate in this research.

Establishing a Relationship with Participants

The relationship between researcher and participants has direct consequences on the "consent process, privacy protections, and scope of data sharing" (Condit et al., 2015, p. 2). The researcher had an existing primitive relationship with potential participants from being a member of several cybersecurity groups and forums. The researcher contacted potential candidates via email, telephone, and social media (Facebook and LinkedIn) services to invite them to take part in the study. The next step was to introduce the identified candidate to the researcher and to explain the purpose of the research on the problem of businesses continuing to fall prey to cyberattacks to candidates via email, phone messages, and social media messages. In the same communication platform, the researcher formally invited the candidate to participate in the research. Candidates were requested to respond regarding whether they met all the eligibility criteria to participate in the research. To acquire more qualified candidates, the researcher employed snowball sampling, a recruitment technique in which participants are asked to assist the researcher in identifying other candidates (Biernacki & Waldorf, 2016). The researcher contacted candidates identified through the snowball technique, using contact information provided by the reference. Also, the initial email, phone messages, or social media messages sent to interview candidates surveyed (a) if the participant was currently working in cybersecurity or information technology roles in U.S. SMBs and (b) if they were between 25 and 65 years old. To be succinct, participants were asked to respond with "Yes" or "No" to each of the questions. Only candidates who answered "Yes" to the questions on the eligibility criteria survey were allowed to participate in the study. After qualified candidates agreed to participate in the study, the researcher scheduled a time and location to interview them. Afterwards, there were a total of 7 IT professionals who participated in the study.

Measures to Ethically Protect Participants

The researcher strictly complied with all policies and procedures of the Institutional Review Board (IRB), established by Liberty University to ensure that the involvement of research participants is well protected. Specifically, identifying information, organizations, and all other details related to candidates and subsequent participants will not be disclosed. Similarly, regarding the data collection process, the researcher limited the data solely to include the information necessary to achieve the objective of the research. Because of the sensitive nature of the cybersecurity field, during the interview process, the researcher did not solicit or purposefully record background information of participants and their business organizations. To ethically protect participants and their confidentiality, the researcher stripped all identifying information from the interview transcripts and final reports and replaced it with non-identifying terminology. More succinctly, the researcher complied with all policies and procedures established by the Institutional Review Board (IRB) for which research data and records will be completely deleted after 3 years.

Research Method and Design

Selecting a research method and design is one of the most crucial decisions. By selecting the appropriate research method and design for a research study, the researcher greatly strengthens the foundation of the study and ensure the achievement of research objectives. More importantly, the research method and design must be suitable for the purpose and problem statements, research questions, conceptual framework, and the review of literature. This section discusses the rationale for choosing the qualitative research method. In addition, this section compares four types of research designs and provides reasons for choosing a case study design.

Discussion of Method

Qualitative research methods assist researchers to examine and explore complex problems or phenomena that have not been researched before or for which the lack of knowledge currently exists (Krathwohl, 2009). The problem addressed in this study was the growing number of cyberattacks critically threatening U.S. SMBs; this problem is one in which the variables and patterns are not all quantifiable. In addition, despite a significant amount of quantitative data about cybersecurity in businesses reported annually and statistical data used in this study, the research regarding the cyberattack pandemic against U.S. businesses is a complicated issue. Indeed, it is an issue for which the outcomes of a quantitative research cannot reveal an in-depth understanding of the current challenges and barriers impacting cybersecurity in businesses (Wolstenholme, 2017). Using qualitative method was more suitable than quantitative method in this study because a qualitative research is more effective in exploring ideas and experiences through words and meanings. Therefore, applying a quantitative research method would be highly insufficient to support the purpose of the study.

Besides quantitative research methods, mixed methods are another commonly used research method. In the field of business, many researchers believe that mixed methods may provide a unique research approach as their research process contains features and characteristics of both qualitative and quantitative methods (Schoonenboom & Johnson, 2017). Nevertheless, employing mixed methods in researching cyberattacks in the business field is considered unreliable because researchers will likely identify the wrong components of the study and the interdependency of quantitative and qualitative elements. As a result, employing mixed methods may mislead the researcher in exploring cybersecurity issues in businesses. According to Nyre-Yu et al. (2019), researchers applying qualitative methods have the advantages of revealing “new

aspects affecting security operations" and uncovering "context-driven insights" of employees working in firms (p. 438). More importantly, during the data collection process, a qualitative research approach enabled participants to share cybersecurity experiences in a more meaningful way, compared to other research methods. Therefore, the use of a qualitative method was the most appropriate for this study.

Discussion of Design

The choice of research design is closely related to research methodology and the problem (Creswell, 2013). There are five types of qualitative methods: narrative, phenomenology, grounded theory, ethnography, and case study. Because exploring the complexity and patterns of the challenges of cybersecurity in businesses requires an in-depth and multifaceted examination, a case study was deemed to be the most appropriate design for this study. In fact, a case study is considered a powerful tool for researchers to study topics related to the fields of business (Crowe et al., 2011). Therefore, conducting a qualitative research with a case study design allowed the researcher to achieve research objectives. In fact, during the data collection process, a qualitative research with a case study design was proven highly effective for extracting valuable data from participants.

Regarding other research designs, they were not chosen due to multiple weaknesses that may mislead the researcher. Despite narrative design being a popular choice in the social sciences field, providing insight into individuals' experiences and the meaning of those experiences, the use of this design to capture the big picture of business' cyber-defense capability could be inaccurate due to distorted information provided by participants (Creswell & Poth, 2018). When using narrative design, the researcher will be required to present participant experiences through personal perspectives (Creswell & Creswell, 2017). As a result, general

public audiences will not be able to fully understand the individual outcomes, as not everyone is familiar with the cybersecurity field. Furthermore, there are two major disadvantages of the phenomenological design preventing the researcher from choosing it (Creswell, 2013). First, finding qualified participants is the foremost challenge, as this design requires participants who share identical experiences, which is not possible for cyber professionals due to the sensitive nature of the cybersecurity field. Second, the grouping process of the phenomenological design can be mistakenly injected with researcher's own biases, which can distort the direction for the research (Tufford & Newman, 2012).

Next, besides being highly vulnerable to researcher bias, grounded theory is considered the most time-consuming research design out of the four qualitative research designs (Timonen et al., 2018). In addition, grounded theory design involves "a multitude of rules that come across as challenging and even obtuse" (Timonen et al., 2018, p. 1). This weakness severely affects both data collection and data analysis. Further, an ethnographic research design is highly ineffective in exploring a multifaceted business problem (Hammersley, 2006). Defining the spatial and temporal boundaries is a big challenge for a researcher selecting an ethnographic design because behaviors of members in any particular group being studied often change unpredictably. In addition, when a researcher is not a member of a group being studied, it is nearly impossible to accurately determining and understanding the context of the study (Creswell & Poth, 2018; Hammersley, 2006). As a result, the single-case study design was deemed to be highly effective for the researcher to explore multiple aspects of cybersecurity in U.S. businesses.

Summary of Research Method and Design

This research effort focused on exploring a greater depth of understanding about the patterns and complexity of an ongoing business problem, a key feature of qualitative study

(Creswell & Creswell, 2017). With an interpretive and naturalistic approach, qualitative method researchers are greatly enabled to investigate participant experiences to produce meaning and insights that can be analyzed and shared with relevant stakeholders to assist them in making better decisions and policies (Creswell, 2013). As the purpose of this study was to explore the problem of U.S. businesses continuing to fall prey to cyberattacks, a case study design was chosen to ensure that the overall objective of the study was achieved. This study design is a great instrument for examining a business through an explanation using multiple perspectives while creating an outline for resolution based on logical analysis (Creswell & Creswell, 2017; van Manen, 2016). For these reasons, the researcher deemed the qualitative research method with a case study design to be the most appropriate for the study of the cybersecurity problems in U.S. businesses.

Population and Sampling

The credibility of qualitative research depends on the appropriate population and sampling selection (Asiamah et al., 2017). As a result, the researcher must carefully define the suitable population and select the proper sampling method and sample size based on research objectives. This section discusses thoroughly the various elements of population and sample size, regarding participants who are working in cybersecurity and IT roles in U.S. businesses. Criteria for the selection of the focus population that represented the current problem with cybersecurity will be presented. Because data saturation is the foundation for any qualitative research (O'Reilly & Parker, 2013), sampling method and sample size will be discussed in detail with respect to addressing the goal of achieving data saturation.

Discussion of Population

For the case study design to be effective, it is crucial for the population to represent the group of individuals sharing similar experiences and characteristics in order for the researcher to accurately identify patterns and themes of collected data (Yin, 2018). In this study, the target population focused on employees currently working in cybersecurity and various IT roles in companies. These job roles comprise the fundamental human resources of both public and private sectors in the long-lasting fight against cyberattacks (Ani et al., 2019; Dawson & Thomson, 2018). Notably, the age range of the target population extended from 25 years old to 65 years old, including both genders. As U.S. businesses are losing billions of dollars to cyberattacks annually (Bernardo, 2015; Osawa, 2017; Paul & Wang, 2019), those companies from which participants were drawn were exclusively from U.S. companies. There were seven participants in this study. They fell under the target population which represents similar experiences and characteristics. Participants were current employees of U.S.-based small or medium businesses.

Discussion of Sampling

Sampling in a case study involves decisions that the researchers make in order to include a selection of knowledge-rich participants to ensure an in-depth study and to achieve their research objectives (Mills et al., 2010). As such, when considering the term “sampling” in this research, the goal was to obtain a sample of the population that could provide representative experiences of employees working in cybersecurity and IT roles to precisely portray the ongoing problem of U.S. businesses suffering from cyberattacks. In fact, choosing the right sample of the target population of interest to examine is the core principle of both qualitative and quantitative research methods (Fowler, 2014). With that being the unchanged principle, regardless of study

methods and designs, it is important to further examine components of sampling. The following sections discuss in detail sampling method, data saturation, and sample size.

Sampling Method. For the study of the ever-increasing number of cyberattacks against U.S. businesses, the chosen sampling method was purposive or purposeful sampling. With this technique, the researcher carefully selected participants based on the purpose of the research, with the expectation that participants would provide valuable knowledge-rich information to the study (Suen et al., 2014). As a result, the sample size is determined by data saturation, and members of the target population are not interchangeable. To be specific, this study employed a homogenous purposive sampling technique. According to Saunders et al. (2012), there are many advantages for researchers using homogenous sampling; cost- and time-effectiveness are the two most commonly cited advantages. Similarly, compared to other sampling methods, purposive sampling with a homogenous approach is a common selection for researchers with studies that have a limited number of primary data sources contributing to the study. Therefore, given the advantages and purpose of this study, purposive sampling with a homogenous approach was a relevant choice for the researcher to strategically conduct this study. The purposive sampling with a homogenous approach resulted in seven participants whose revealed information reached data saturation.

Data Saturation and Sample Size. "Data saturation is reached when there is enough information to replicate the study, when the ability to obtain additional new information has been attained, and when further coding is no longer feasible" (Fusch & Ness, 2015, p. 1408). In fact, failure to reach data saturation has a severe impact on research quality and content validity (Fusch & Ness, 2015). Data saturation and sample size are closely related by an interdependent relationship. "Sample size is justified by interviewing participants until reaching data saturation"

(Francis et al., 2010, p. 1229). In other words, the sample size is determined by the researcher determining when data saturation is reached. According to Creswell (2014), sample size varies by research design, which ranges from two to 30 participants. This research study reached data saturation at the 7th participant. Therefore, the total sample size was seven interviewees. Regarding the case study design, Creswell (2014) examined multiple qualitative research studies and found that a qualitative researcher requires "about four to five cases [participants]" for data saturation (p. 189). Contradictorily, Guest et al. (2006) found that, despite collecting data from 60 participants, they had data saturation at 12, with most emergent themes at 6. Similarly, researchers are recommended to use a sample size between 6 to 12 participants so that not only data saturation can be reached but also diversity of experience can be attained. Interestingly, Mason (2010) examined hundreds of doctoral theses relying on qualitative methods and concluded that data saturation is often achieved with a target population of 10 participants. As the sample size for data saturation discussed in several studies varies, it is crucial for the researcher to determine the sample size based on when data saturation is reached to assure validity of the research, rather than predetermine a specific number of sample size. For this qualitative research study, the researcher determined that data saturation was reached at the 7th interviewee as there were no new emergent themes.

Summary of Population and Sampling

Population and sampling are two foundational components for the research on the increasing cyberattacks against U.S. businesses. In this study, the target population was employees who were currently working in cybersecurity and IT roles in U.S. businesses with an age range from 25 to 65 years old. With the criteria for focus population established, the researcher deemed purposeful sampling with a homogenous approach as the most suitable for

this study. It is important to note that data saturation is a vital objective that the researcher must achieve in the data collection process through target population, sampling method, and sample size. From the target population and purposive sampling method, the data collection reached saturation with seven participants.

Data Collection

The goal of a qualitative research with a single-case study design is to answer the how and why questions of a subject (Yin, 2018). Therefore, the data collection process is one of the most crucial elements to achieve research objectives. In order to collect data accurately, specific data collection techniques were utilized to capture the context-driven insights and information of cyber professionals on cybersecurity problems in U.S. businesses. This section details the data collection process and its elements. More specifically, the instruments for data collection, data collection technique, and data organization technique are discussed in depth.

Instruments

In a qualitative study with a case study design, the researcher serves the role of an active participant in the process of data collection (Creswell, 2014; Stake, 2010). There are two primary tasks involved in data collection. They are audio recording interviews and taking notes. The intent of these two crucial tasks is for the researcher to not only record verbal information but also to capture behavioral cues. This section discusses the researcher as an instrument of the study, interviewing and audio recording, interview guide, and notes.

The Researcher as an Instrument of the Study. "The researcher's thinking lies at the heart of the inquiry" (Piantanida & Garman, 1999, p. 24). With this principle, the researcher was one of the instruments of this study. Indeed, in the data collection process, the researcher serves as the decision-making instrument that decides the method and design of the research. This

instrument is responsible for the specific stages and procedures for the data collection process that directly impacts the research outcomes. Furthermore, as the researcher is a participant in a qualitative study, in this case a single-case study, necessary measures must be taken to safeguard against bias (Chapman, 2014). To safeguard against personal bias, the researcher developed a personal journal, laying out thoughts and personal experiences related to the study. Specifically, the personal journal was a means for the researcher to capture his thoughts and experiences in the field of cybersecurity. The journal bracketed out researcher biases and helped him to remain open to descriptions and information provided by participants (Piantanida & Garman, 1999). In short, the researcher was an instrument of the study by means of deciding the method and design of the research and was responsible for taking appropriate measures to prevent biases from impacting the study outcomes.

Interviewing and Audio Recording. The method for data collection in this study was interviewing participants. For all qualitative research employing this method, the process of interviewing depends on the researcher accurately capturing and reporting participants' responses with audio recording and verbatim transcription (Jamshed, 2014). Corbin and Strauss (2014) recommended that for in-depth interviews, researchers should structure and rely on semi-structured interviews where participants answer planned, open-ended questions. As such, semi-structured interviews were employed for this study. Indeed, this data collection method better assisted the researcher in acquiring in-depth responses on organizational and technical barriers for improving cyber defense and both technical and non-technical defense mechanisms. Particularly, semi-structured interviews involve less restrictions and participants are allowed to give more productive information and perspectives (Marrelli, 2007). This means that acquired

responses shed more light on the problem of U.S. businesses continuing to fall prey to cyberattacks.

Interview Guide. Textual and structural description of cybersecurity and IT professionals' interviews who were employed in U.S. businesses was the foremost goal of the interview process. With that being the goal, Appendix A contains the schematic script with strategic flow to interview participants. More succinctly, it comprises an introductory statement, interview questions related to the research questions, and a closing statement. The introductory statement is a means for participants to feel comfortable and an opportunity for the researcher to make impressions and affirm the purpose of the study to participants (Creswell, 2014). Although the research questions were well structured and strategized, it is important to note that the script during the interview process could change depending on the responses of the participants. By doing so, the researcher could acquire from these cyber professionals as much information about cybersecurity in U.S. businesses as possible. In other words, the researcher asked follow-up questions for additional insights or clarification, with the objective of generating richer responses regarding cybersecurity in U.S. businesses. Finally, the closing statement is an opportunity for the researcher to show appreciation to participants and remind them to later contact the researcher if they have any concern, comments, or clarification.

Notes. Besides the verbal information acquired from participants in interviews, contextual cues or behavioral cues cannot be overlooked while interacting with interviewees. Indeed, Marrelli (2007) recommended that case study researchers "record the exact" nonverbal forms of communication while asking interview questions (p. 43). As the researcher intended to record nonverbal communication factors of interviewees, it was a crucial role for the researcher to take field notes and keep track of nonverbal elements, which were impossible to capture by

audio recording. By capturing nonverbal elements, the researcher gains the depth and explores the richness of key issues. To assist with data analysis and the study purpose, notes were integrated into the interview transcript.

Data Collection Technique

Ethical Responsibility of the Researcher. Cybersecurity is a highly sensitive topic for cyber professionals to disclose to outsiders. Therefore, it is the ethical responsibility of the researcher to protect and maintain both acquired data and information of participants. Specifically, Marrelli (2007) mentioned that the researcher must protect "subjects from embarrassment, loss of self-esteem, reduced standing in their community, or risks to their employment" (p. 43). Indeed, leaking information acquired from a participant on a company's cyber vulnerability would not only result in that business becoming a cyber victim but also severely impact the employment and cyber-community standing of that cyber professional. In fact, this was the concern of some participants and the researcher was able to ensure participants that their confidentiality would be protected, which encouraged them to take part in the data collection process. Therefore, the researcher strictly upheld ethical standards of protecting confidential information by removing as recommended, defining the limits of access of interview questions, and avoiding seeking information about specific technical cyber vulnerabilities.

Collection Process. A well-planned set of questions was utilized to explore the current problem of cybersecurity in U.S. businesses. These questions served as a guide for the researcher to evoke knowledge-rich responses from cyber professionals throughout the interview process. Notably, there were some questions that evolved from planned questions or were eliminated as the participants shared their experiences and insights. This approach was exceptionally crucial to the study, as the circumstances of cybersecurity vary among different companies and multiple

factors, both technical and non-technical, affect organizational cyber vulnerabilities (James, 2018; Nobles, 2018). As a result, this data collection technique achieved the diversity of thoughts and information of data collection. With the less restrictive nature of a semi-structured interview, it allowed 7 cyber professionals to share more in-depth details through probing and follow-up questions. To establish the initial relationship with participants, the researcher made initial contact and invited candidates to participate in the research. For candidates who declined to join the research, they were asked to refer other qualified candidates who could be a part of the study. Because both confidential information and security for participants and their business organization were the foremost ethical standards, the researcher protected all identifying information. All confidential information will not be disclosed. To ensure this, the sensitive information was extricated from the acquired data.

Collecting Participant Data. For the 7 candidates who agreed to join the study, the researcher asked them to select a preferred method such as telephone, face-to-face, or a video call app for interviewing and location. This ensured convenience and comfort for the participants. When participants confirmed their preferred method and location, the researcher scheduled the interview. It is important to note that the participants were working employees; therefore, the researcher accommodated their suggested schedules. The main instrument to collect participant responses was audio recording. After each interview, the audio recording was transcribed into a Microsoft Word document along with noted behavioral cues. The researcher contacted participants to review and ascertain that the verbatim transcriptions of their interviews were accurate.

Data Organization Technique

Audio recordings and notes capturing nonverbal cues were the two fundamental types of data to be safely secured. After each interview, the researcher safely transported and securely stored the recording device containing the audio record and interview notes. Then, the audio record was transcribed into a Microsoft Word document along with interview notes at the researcher's safeguarded house. During the transcribing process, all identifying data were removed to assure confidentiality. All files, both copied and original, will be saved in the highly secured file location protected by encryption. To comply with Liberty University's Institutional Review Board, data will be maintained for a specific period, then completely destroyed.

Summary of Data Collection

A qualitative research with a case study design cannot achieve its study objectives without the data collection process. In fact, the reliability and validity of a research depend partially on the process of data collection (Creswell & Creswell, 2017). Therefore, the process of data collection in this research study included interviews and audio recordings, notes on nonverbal communication, and an interview guide. Additionally, the technique of data collection is also examined, in which the responsibility of the researcher in protecting participants' confidentiality, details of steps for collecting data, and interactions with participants before and after interviews is strategized. Finally, the researcher lays out procedures for organizing the collected data, protecting data security, storing acquired data, and actions taken to safely dispose of data.

Data Analysis

According to Creswell and Poth (2018), the objective of data analysis is to summarize, analyze, and interpret collected data to explore patterns and relationships of a research subject.

This section discusses the details of the analysis method and coding process. For the analysis process, the researcher employed the thematic analysis method to ensure the trustworthiness of research outcomes. The thematic analysis method, in particular, was deemed suitable for exploring themes concerning cyberattacks against U.S. SMBs through six phrases. More succinctly, the coding process of the thematic analysis method is considered the most critical procedure for data analysis and research objections (Belotto, 2018). The process of coding data in this study contained two stages: initial coding and expanded coding. In addition, the researcher applied the deductive approach during the coding process. With this in mind, the analysis method section will discuss the analysis method and coding process in detail.

Analysis Method

For a qualitative research study to be accepted as trustworthy, data analysis must be conducted in a precise and consistent manner (Nowell et al., 2017). This study attempted to identify elements of the problem of U.S. SMBs continuing to fall prey to cyberattacks. Therefore, this study required an analysis method that has the ability to examine and analyze collected data for linked passages in order to provide a thorough description of the problem being studied. The thematic analysis method was deemed suitable for exploring cybersecurity issues that businesses are facing, as this method is "a method for identifying, analyzing and reporting patterns (themes) within data" (Braun & Clarke, 2006, p. 79). In fact, "thematic analysis provides a purely qualitative, detailed, and nuanced account of data" (Vaismoradi et al., 2013, p. 400). For the study of the ever-increasing cyberattacks in U.S. SMBs, the researcher followed data analysis phases recommended by Vaismoradi et al. (2013) to produce trustworthy and insightful findings. There are six phases for a thematic analysis to thoroughly evaluate and examine data: familiarizing with data, generating initial codes, searching for themes, reviewing

themes, defining and naming themes, and producing the report. In these phases, coding is considered one of the most crucial processes as it has the biggest impact on both data analysis and research outcomes (Belotto, 2018). The data analysis process in this study concentrated on the coding process using issues identified in the problem statement to identify emerging themes of cyberattacks against U.S. SMBs. In the end, there were a total of 13 themes discovered.

Coding Process

This study relied on coding to identify themes and patterns for the problem of U.S. businesses continuing to fall prey to cyberattacks. Coding is considered the universal process used in qualitative research**,** in which the researcher breaks down acquired data before putting back together with the goal of discovering breakthrough information (Elliott, 2018). In fact, coding enables the ultimate goal**s** of a case study**,** which are to "uncover patterns, determine meanings, construct conclusions and build theory" (Patton & Appelbaum, 2003, p. 67). Additionally, this process ensures the reliability and consistency of the research (Elliott, 2018). In this study, the coding process comprised two stages: initial codes and expended code. Atkinson (2002) believed that these two stages are the fundamentalities for any case study**,** enabling researchers to associate meanings of chunks of data with patterns and themes from the focus population. The researcher generated an initial set of codes based on collected data by taking into consideration the research questions and key areas. As suggested, the initial codes structure the foundation for a more thorough organization and classification of coded data in order to accurately identify patterns and themes (Marrelli, 2007). This then allows the researcher to conduct expanded coding. In expanded coding, the researcher must rationally and logically group data for particular themes by examining chunks or segments of data. At this point, the synthesis and interpretation process begins, as the researcher utilizes patterns and themes to write

about the description and breakthrough information that could initiate changes in business organizations to defend against the ever-increasing number of cyberattacks in the business sector.

Coding Approach. Codes are driven by collected data and research theory, through either the deductive or inductive approach to identify patterns (Xu & Zammit, 2020). With a deductive approach, the researcher formulates a codebook or pre-set coding schemes to use as a reference guide through the coding process (Fereday & Muir-Cochrane, 2006). On the contrary, a researcher with an inductive approach builds and modifies codes from data throughout the coding process. For the study of the ever-increasing cyberattacks in U.S. SMBs, a deductive approach was considered the more applicable approach. Specifically, the researcher created an exhaustive list of pre-defined codes based on a review of the literature, elements of the problem and purpose statement, and how participants referred to a topic (Mihas, 2019). With the deductive approach deemed suitable for this research study, the researcher utilized a list of pre-defined codes for reference in the coding process and guidance to make sense of data.

Coding Tool. For any given research, manual text coding and computer-assisted coding are the two prime choices (Ktari, 2010). For this research study, a computer-assisted coding tool was employed to identify themes from collected data. Specifically, the researcher used NVivo software to facilitate annotation of the text within the data and for the discovery of emergent themes. According to Ktari (2010), computer-assisted coding is highly effective for the researcher in saving time and effort and relieving the burden of concentrating on coding. However, computer-assisted coding has a major weakness of being applicable for simple content only (Jones et al., 2014). This weakness means that ironic texts and underlying meaning could be ignored during the coding process. Therefore, with the coding process relying on NVivo

software, the researcher actively interfered with the computer-assisted coding. Specifically, Ktari recommended the active role of the researcher in "identifying the concepts to be coded, determining the level of generalization, and creating the translation rules" (p. 7). In short, the researcher used NVivo software for the coding process while actively interfering with all phrases of the coding process in order to ensure the in-depth examination of collected data.

Summary of Data Analysis

The process of data analysis and coding were discussed in this section. Specifically, thematic data analysis with six phases was chosen as the procedure for identifying themes and patterns of cybersecurity problems in U.S. businesses. In the coding process, the researcher conducted two stages, initial coding and expanded coding, to provide an accurate interpretation of collected data. Using the deductive coding approach, a list of pre-defined codes was built based on the review of literature and elements from the problem and purpose statements of this study. To better assist with the coding process, the research proposed the use of NVivo software. With the use of computer-assisted coding, the researcher followed the recommendation of Ktari (2010) to actively interfere in the coding process to ensure that all in-depth information was examined.

Reliability and Validity

A research study is deemed worthless without reliability and validity. In other words, reliability and validity are the two methodological concepts measuring and evaluating the quality of a research based on several objectives that the researcher must achieve (Creswell & Poth, 2018). Therefore, this study applied appropriate measures in the process of data collection and data analysis to ensure the reliability and validity of research outcomes. More importantly, the researcher had the crucial goal in ensuring the study to be reliable and valid. This section

provides details of steps taken in the process of data collection and data analysis and the role of the researcher to establish reliability and validity in the study of the ever-increasing number of cyberattacks against U.S. SMBs.

Reliability

In qualitative research, reliability is established by the consistency of a measure and the approximate degree of multiple assessments in a study (Syed & Nelson, 2015). Krippendorff (2004) characterized reliability in research as consisting of three criteria: stability, reproducibility, and accuracy. With reliability defined, for a qualitative research to be considered reliable, the researcher must seek consistency in the study method utilized in data collection and analysis. After discussing the lack of reliability in several qualitative research studies, Noble and Smith (2015) recommended that the qualitative researcher should establish a clear and meticulous decision trail throughout the research process that explicitly details decisions taken for methodological and analytic choices. This means that method selection and elements in the process and procedures of data collection and analysis must be precisely documented, to not only ensure the utmost reliability of the study but also to provide readers with consistency in research findings. Accordingly, the researcher followed the recommended approach to achieve reliability in the research process.

Furthermore, as recommended by Creswell and Poth (2018) for improving reliability in qualitative studies, the researcher obtained detailed field notes by using high-quality audio recording devices and by accurately transcribing the recorded files. The goal was to present an interviewee's unmodified response to each interview question in the final report with truthfulness and consistency of data. More succinctly, the interview guide is a great instrument addressing reliability. Conway et al. (1995) suggested that the researcher must structure and standardize the

interview guide from a neutral position free from personal biases and prejudgments, so that the interview questions do not lead participants to answer in the researcher's preference. While employing the interview guide during the interview process, the researcher serves as the most critical instrument for maintaining consistency by following the guide and procedures for all participants. Notably, because the semi-structured interview was the chosen method in this study, the researcher asked similar follow-up probing questions of all participants, to maintain consistency of data throughout the interview process. Regarding data analysis, Creswell and Poth pointed out that when there are too many coders, the analysis process will be smeared, resulting in complications and misleading outcomes. Following this caution, the researcher was the only person engaging in the data collection process, coding process, and analysis procedures. More importantly, the researcher consulted with faculty members at Liberty University to ensure the reliability of this research study. The researcher assumed that the expertise and competence of faculty members accurately assessed the stability, reproducibility, and accuracy of the study of the ongoing problem of growing cyberattacks in small and medium enterprises.

Validity

Saturation. Data saturation is reached only if no new information emerges (Creswell & Poth, 2018; Yin, 2018). The researcher recognizes that data saturation is achieved "when further coding is no longer feasible" and "when there is enough information to replicate the study" (Fusch & Ness, 2015, p. 1408). In qualitative research, data saturation is fundamentally deciding whether a research has validity**,** which relates to its practical contributions to the field being studied (Francis et al., 2010). Data saturation is a pillar of qualitative research because, as opposed to quantitative research**,** which seeks generalizability of findings, qualitative research is concerned less with sample size but focuses more on appropriateness and validity of data

(O'Reilly & Parker, 2013). To ensure the validity of this study, the researcher only stopped collecting data at the 7th participant when data saturation was reached. Specifically, when no new information or themes were discovered during the interview process of the 7th participant, the researcher was signaled to cease data collecting. Therefore, the data collection process of this research prioritized the saturation of collected data to maximize the validity of the research after thoroughly collecting data from seven participants.

Triangulation. According to Creswell and Poth (2018), the credibility and validity of a research are established by the triangulation process. This process entails the use of multiple methods and information sources to formulate the comprehensive understanding of the study (Carter et al., 2014). In this study, triangulation was achieved through the extensive review of literature, in-depth information acquired from seven participants coming from various roles in cybersecurity and IT in different businesses, and comparisons of themes during the data analysis process. Besides discussing relevant concepts of cybersecurity in business, the literature review section in this study not only provided the conceptual contribution and the contemporary circumstances of cybersecurity in U.S. businesses but also served as the additional fundamental source assuring the validity of the research. In fact, Yin (2014) highlighted that for any qualitative research employing a case study method, the section of literature review is a substantial instrument for data triangulation. Specifically, a literature review section of a qualitative research is a part of data triangulation because this section cross-validates data and captures diverse dimensions of a subject. With the same intent, data triangulation is achieved organically during the data collection and analysis process. Regarding the study on the ever-increasing number of cyberattacks against U.S. SMBs, participants came from different functions of cybersecurity and IT roles. These participants were employed in distinct companies with

different types of information systems and cyber capacity; each participant provided distinct responses and insights that make up the diverse dimensions of the increasing cyberattacks in U.S. businesses. Additionally, during the data analysis process of seven participants, emergent themes and patterns were compared strategically and analyzed logically. By doing so, the researcher provided the additional attribution to data triangulation of cybersecurity in U.S. businesses. In summary, data triangulation for research validity is achieved through three thoroughly strategized components: the extensive literature review, diverse background and roles of participants, and strategic comparisons of the data analysis process.

Summary of Reliability and Validity

This section discussed the role of reliability and validity in qualitative research. As illustrated, without reliability and validity, a research study has no quality and applicability. Importantly, there are strategies that the researcher could take to ensure that the study on the problem of the increasing cybersecurity attacks against U.S. businesses was valid and reliable. For reliability, the researcher employed high-quality field notes, recording devices, and interview guide to ensure that the outcomes of this study were reliable. In addition, the researcher strategized follow-up and probing questions during the interview process to ensure the consistency of the study. Furthermore, a valid research study comprises of data saturation and triangulation (Creswell & Poth, 2018; Yin, 2018). To achieve data saturation in this study, the researcher conducted data collection until no new themes emerged for which 7 IT professionals were interviewed. For data triangulation, the researcher relied on the review of literature section in this study, in-depth information acquired from diverse participants, and comparisons of data and themes during the data analysis process.

Transition and Summary of Section 2

This section summarizes and concludes Section 2: The Project, which establishes the framework and foundation for the exploration of the increasing cyberattacks against U.S. businesses through cyber professionals currently working in cybersecurity and information technology roles. In the beginning, the purpose statement was reexamined. Next, the role of the researcher section detailed the involvement of the researcher in conducting the study, which comprises designing the research, collecting and maintaining acquired data, and conducting data analysis. Following, the section on participants addressed steps and procedures to gaining access to participants, establishing a relationship with participants, and identifying measures to ethically protect participants. In any qualitative study, research method and design serve as the primary instrument to achieve the successful outcomes of the study. In the research method and design section, the chosen method and design were identified and justified for their application in this study. In short, this study employed a qualitative method with a case study design.

There was a total of 7 IT professionals participating in this study, who were in the focus population. The focus population was employees currently working in cybersecurity and information technology roles in U.S. business, with ages ranging from 25 to 65. The sampling method section provided details on sampling method, data saturation, and sample size. After that, the data collection section describes instruments for data collection, data collection technique, and data organization technique. The intent of these aforementioned methods is to acquire the most context-driven insights and information from participants, choose the suitable technique for collecting data, and establish steps for organizing and securing acquired data. As raw data is collected, it is important to conduct data analysis. Data coding in the data analysis section detailed the steps for coding and interpreting the data that will be collected. More importantly,

the section on reliability and validity discussed the significant role of having valid and reliable methods and strategies that the researcher needs to take in order to ensure reliability and validity. Specifically, this section offered great insight and details with respect to consistency, saturation, and triangulation.

The framework and standards for exploring cybersecurity issues in U.S. businesses were established in Section 2: The Project. The next section, Section 3: Application to Professional Practice and Implications for Change, will present and discuss research findings through analysis of collected data. In addition, the applicability of the findings will be discussed. More importantly, the researcher will present recommendations for actions that U.S. businesses should take regarding the increasing cyberattacks against them. Section 3 will conclude with reflections of the researcher.

Section 3: Application to Professional Practice and Implications for Change

This section begins with a brief overview of the study of the ever-increasing number of cyberattacks in U.S. small and medium businesses. The overview of the study reviews the why and the how questions of the issues of cybersecurity in U.S. business sector. Next, the section on presentation of the findings discusses findings derived from collected data that address the six research questions posed in this study, as well as data discrepancies. The presentation of the findings section provides a detailed discussion of discovered themes and links each theme back to the conceptual framework and literature review in this research. Furthermore, the application to professional practice section provides a thorough discussion on the applicability of the findings in the context of U.S. SMBs, as well as recommendations for actions. For future studies, the recommendation for further study section reviews crucial elements that should be focused on in further research studies, based upon the findings of the present study of the growing number of cyberattacks against U.S. SMBs. Last, the study ends with reflections of the researcher and a summary of the application to professional practice and implications for change.

Overview of the Study

The researcher utilized a qualitative research method to reveal the contemporary barriers and challenges that are impacting cybersecurity competencies of U.S. small and medium enterprises. A single-case study design with a semi-structured interview data collection technique was employed to collect data from cyber professionals currently working in small and medium businesses across the United States. The purpose of this research design was to determine impacts of technical barriers, business strategies, and organizational elements resulting in cyber vulnerabilities that cause businesses to become cyber victims. Existing research addressing both business and cybersecurity fields pointed out that the loss due to cyberattacks of U.S. small and

medium business will continue to rise (Paoli et al., 2018; Tagarev et al., 2017). This gloomy foreseeable reality is the result of the current primitive technical infrastructure and organizational nature of small and medium businesses (FBI News, 2020; Hawkins, 2017; Kaspersky Lab, 2017; Srinidhi et al., 2015). The sampling technique in this study was purposive sampling with a homogenous approach that was highly advantageous for studies with a limited number of primary data sources. The data collection cycle is shown in Figure 2. To collect data for this qualitative study, the researcher contacted working cyber professionals via emails and social media messaging services to invite candidates to participate in the study. The researcher introduced the purpose of this study, then invited candidates to participate and surveyed them with questions for eligibility criteria. All participants in this study signed the consent form and agreed to fulfill their role in this research. Participants were available and willing to clarify collected data after the conducted interviews. The ideal sample size for qualitative research with a case study design is between 4 and 10 cases or participants (Creswell, 2014; Guest et al., 2006; Mason, 2010). The researcher determined that data saturation was achieved after the seventh interviewee when there was no new information revealed. The participants' genders are displayed in Figure 3.

Figure 2

Data Collection Cycle

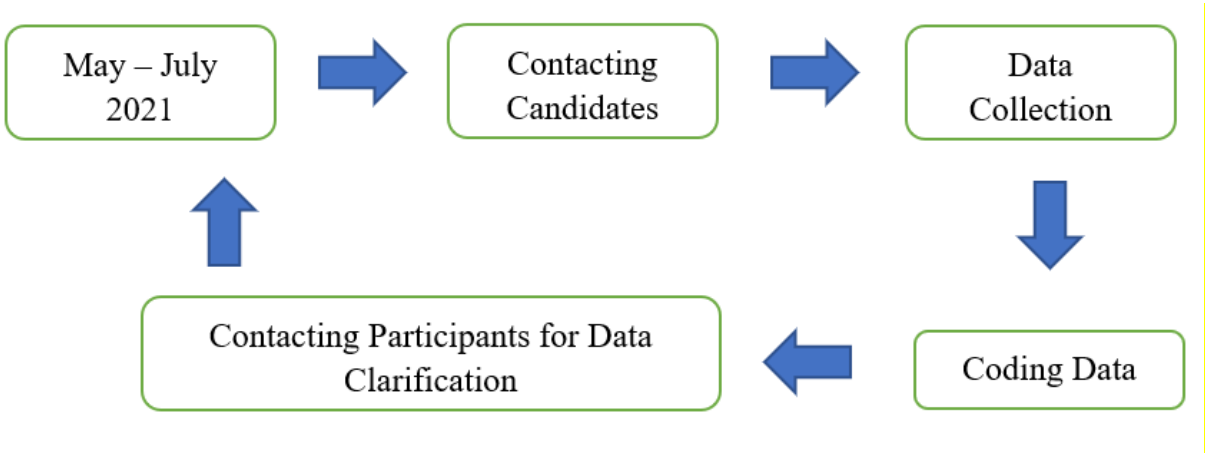
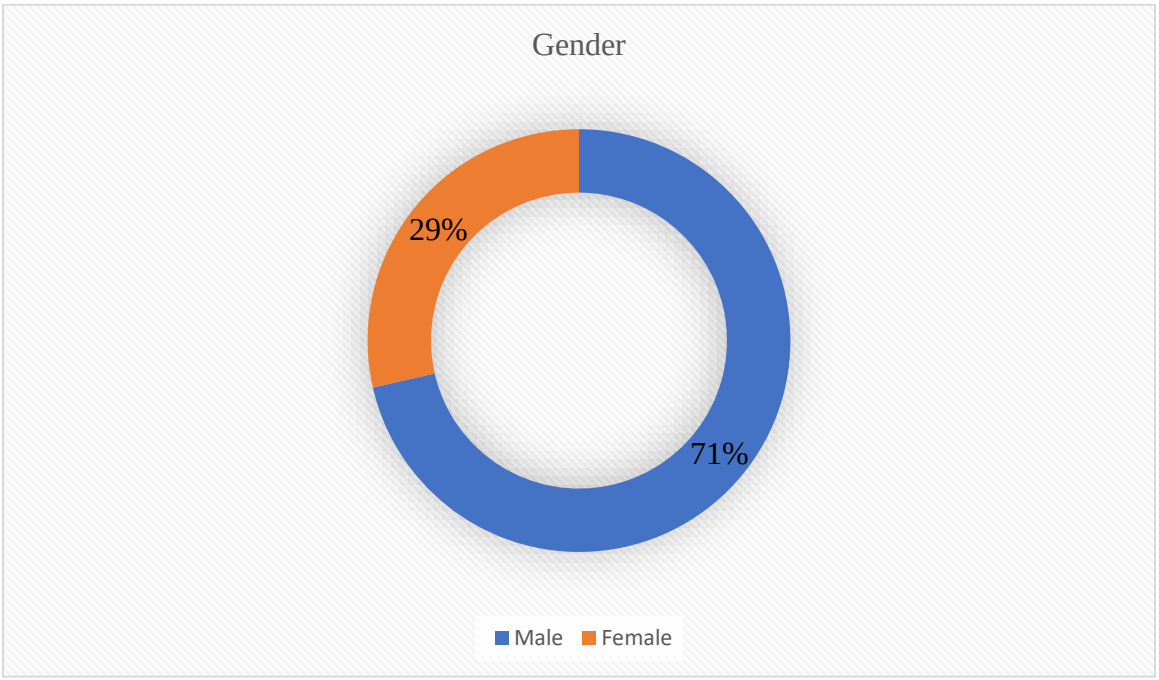


Figure 3

Gender of Participants



Anticipated Themes

There were three potential themes identified after reviewing the existing literature addressing cybersecurity in U.S. businesses. The first theme focused extensively on the damages of cyberattacks and their common methods. Alarmingly, cyberattacks cost U.S. businesses billions of dollars annually (Gordon et al., 2015; Wang, 2019). In detail, this cost includes both the damages of cyberattacks (Paoli et al., 2018; Tagarev et al., 2017; Wang, 2019) and expenses for investing in a more secure cyber defense due to past attacks (Krishan, 2018; Musman & Turner, 2018; Srinidhi et al., 2015). Even more importantly than the monetary value that cyberattacks destroy in their aftermath, victimized businesses also endure the damages to reputation and customer trust (Information Systems Audit and Control Association [ISACA], 2019a, 2019b; Morse et al., 2018; Pharris, 2019). This destruction is immeasurable and long-lasting, as it takes considerable time and effort for victimized businesses to recover to the pre-attack condition (Heikkilä et al., 2016). Inevitably, in the recovery process, businesses often change their operational procedure, which could cause further disruption to the customer base (Deane et al., 2019). As a result, losses of U.S. businesses due to cyber breaches rise dramatically every year (FBI, 2018).

The second anticipated theme pertained to cyber defense in U.S. small and medium businesses. Ideally, a proactive defense system is the optimal choice for businesses, rather than an active or passive defense system (Byres, 2014; Lai & Wu, 2015; Wagner, 2016). A proactive defense system in any organization requires three crucial components: defense in depth, understanding the threats, and routine checkups for hardware and software (Byres, 2014; Nam, 2019; Presher, 2015; Wagner, 2016). It is important to note that any U.S. business missing one of four stages of defense capabilities is more vulnerable to cyberattacks (Clay, 2015; Korba et al.,

2016; Nagurney & Shukla, 2017; Taitto et al., 2018). The four crucial stages of defense capabilities are: prepare, prevent, detect, and respond. Importantly, annual data reported by the FBI (2018) indicated that cyber breaches in U.S. small and medium businesses are nearly unstoppable. This leads to the vital requirement for cyber-risk management, which centralized on identifying risks and vulnerabilities and implementing strategic changes (Hayes & Cappa, 2018; Král & Králová, 2016; Qassim et al., 2019; Scholz et al., 2020; Sonenshein, 2010; Ukil & Akkas, 2017). In addition to the vital role of cyber-risk management in U.S. small and medium businesses, the anticipated themes revealed from previous literature indicate that there are deadly cyber weaknesses existing in U.S. small and medium businesses. Evidently, the lack of security training, lack of security skills, and negligence in safeguarding critical infrastructure are the three roots of cyber vulnerabilities in many small and medium businesses (Caldwell, 2016; Cameron & Marcum, 2019; Hanus & Wu, 2016; Hayden, 2015; Kennedy, 2016; Smith, 2018).

Raising cyber awareness, improving defense to prevent being a cyber target, and incorporating cybersecurity into business process is the third anticipated theme. Findings in the literature indicate that by combining all three measures, U.S. small and medium businesses will not only become less of cyber targets but also significantly improve business process and productivity (Azhagiri et al., 2017; Hadji-Janev & Bogdanoski, 2017; Homoliak et al., 2019; ISACA, 2012a; Rubino et al., 2017). This anticipated theme involves a wide range of business elements to improve both technical and non-technical segments of business cybersecurity capability. These significant elements are human resource development, leadership, strategic investments, business-specific defense mechanisms, business environment, enterprise end-to-end process, and business governance and management (Friedberg et al., 2015; He & Zhang, 2019; Hu et al., 2018; ISACA, 2013; Jugdev, 2019; Kemper, 2019). Alarmingly, this third anticipated

theme revealed the fatal weaknesses of small and medium businesses in the battle against cybercriminals due to many uncontrollable and organizational factors such as skill shortage, budget constraints, resistance to organizational changes, and reliance on irrelevant business framework (Dawson & Thomson, 2018; Devos & van de Ginste, 2015; Lee et al., 2015; Slayton, 2017).

Presentation of the Findings

The findings of the study of the ever-increasing cyberattacks in U.S. SMBs indicated that business organizations disregard the significant threat and overwhelming risk of cyberattacks against their technological infrastructure. Despite being increasingly dependent on data and technology in daily operation, improving cyber-defense capability is not the priority for U.S. SMBs. Furthermore, the findings of this study revealed the crucial indication that technological factors are not the only Achilles' heel of managing cyber defense in businesses but also organizational elements. Notably, responses from cyber professionals who participated in this study showed that U.S. SMBs focus on defending themselves digitally only after they have been victimized. The following section will explain at length the findings regarding cyber capability in U.S. SMBs.

Table 1

Themes Discovered in the Data Analysis Process

Theme Number	Study Themes
Theme 1	Technology Deficiencies
Theme 2	The Advancement of Technology
Theme 3	Lack of Knowledge
Theme 4	Problems of Human Resources
Theme 5	The Lack of Investment in Cybersecurity
Theme 6	The Human Factor Is the Weakest Link
Theme 7	The Less Training and Support, the More Depleted Cybersecurity Capability
Theme 8	Security Policies
Theme 9	Obsolete Technological Infrastructure
Theme 10	Outsourcing Cybersecurity
Theme 11	Bring-Your-Own Devices: Policy and Network Segmentation
Theme 12	Conducting Evaluation on Risks from Third Party
Theme 13	Cultivating an Organizational Culture for Cybersecurity

Themes Discovered

This section presents themes discovered during the data analysis process. Through collecting data from multiple participants, there were a total of 13 themes discovered; see Table 1. Discovered themes covered, more than expected, the urgent matters that currently exist in both the cybersecurity field and the business field. Related to the purpose and the problem being

studied, discovered themes exposed multiple technological and organizational elements of cyber defense in U.S. SMBs and the connections between those elements. With that being put forward, the section presents themes discovered through an analysis of the experience and knowledge of employees currently working in U.S. SMBs.

Research Question RQ1 Themes. Research question RQ1 was "why do small- and medium-sized businesses increasingly fall victim to cyberattacks?" There are many reasons for SMBs to increasingly fall victim to cyberattacks. From collected data, the causes of this cyber pandemic are originated from both external and internal environments of SMBs. Succinctly, participants approach the problems of atrocious cyber defense in SMBs through three points of view. They are the condition of technology in businesses, the technology development in the field of technology, and the organizational challenges. From there, there were three themes discovered: technology deficiencies, the advancement of technology, and the lack of knowledge.

Theme 1: Technology Deficiencies. Technology deficiencies are considered one of the most impactful drivers for the increasing number of U.S. SMBs falling victim to cyberattacks. Indeed, most cyberattacks are supported by up-to-date technology with advanced knowledge, as each attack requires perpetrators to be one step ahead of the intended victims to carry out the attack ("Recent Cyberattack Raises Alarm," 2020). Disturbingly, all participants stated that businesses they have worked for, including the small and medium companies where they are currently employed, have technology deficiencies ranging from software and hardware to physical controls. In many instances, participants explained that from the perspective of small and medium business, organizations feel more comfortable using the technology that has been used for years. Similarly, constraints of financial resources and knowledge are preventing small- and medium-sized companies from improving this cyber weakness.

Participant 2 discussed his overwhelming challenges of the dated computer systems he encountered during the first year working for a small business organization, as well as his doubt of the foreseeable cyberattacks against the company's cyber structure. Furthermore, Participant 2, a cyber professional with years of experience, recalled his first impression when he started working for the small business, that "the technology the company is using either outdated or isn't right for their business." He realized that being the only cyber professional in the company, it would require years to improve the current state of technology deficiencies at the company. Noticeably, Participant 4 expressed that the outdated technology was a significant burden for him, as he could not fulfill his job function. This sentiment was shared by Participant 5 as well, as he stated that "it is stressful that people are waiting for you and your computer is barely working, the app keeps crashing." All participants conceded that solving technology deficiencies at their business organizations is a necessity for daily operation and cyber capability, as they believed similarly to Participant 1, who emphasized that "there is bad guys out there, if they want to take advantages of [company name] decade-old computer and network, there is nothing that can stop them. We are just waiting for disaster to happen." Thus, to avoid being the next cyber victims, U.S. SMBs must resolve their deadly weakness: technology deficiencies.

Theme 2: The Advancement of Technology. The advancement of technology helps businesses to improve their business process, communication, and activities. Nevertheless, technology advancement has more negative influence on U.S. SMBs than positive influence, according to responses from participants. From the perspective of participants, large companies and corporations have more benefits from the advancement of technology than businesses of small and medium size. Interestingly, many participants discussed that the advancement of technology widens the market competition gap between corporations and SMBs because the

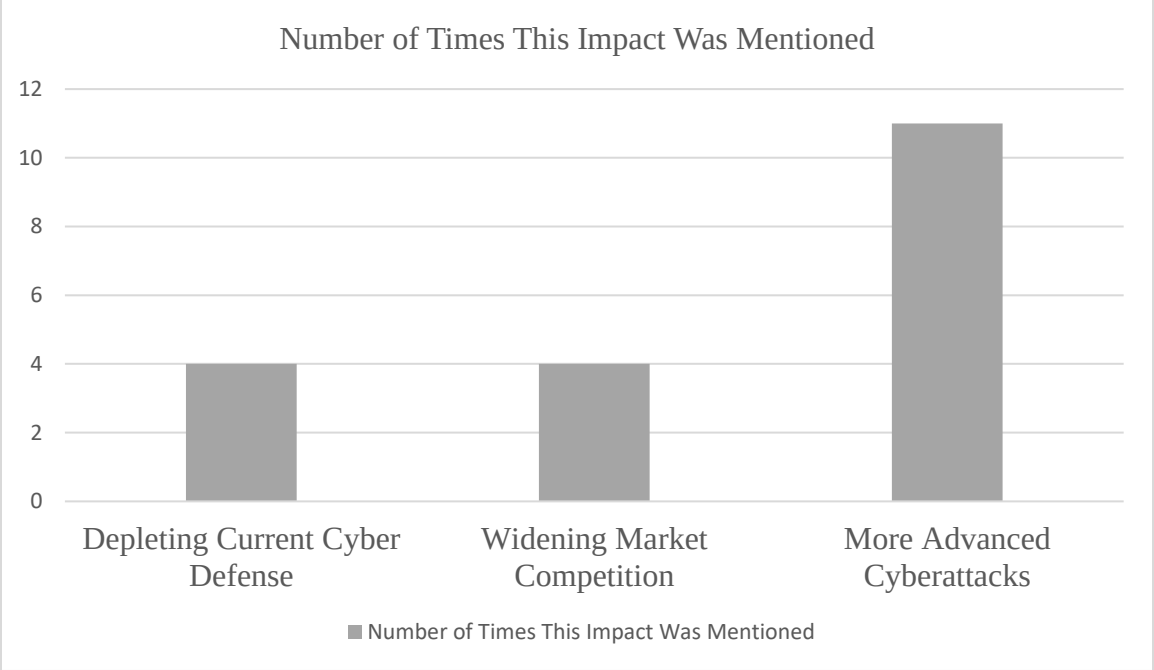
larger a business organization is, the more financial and human resources are available to upgrade technology capability and more customer bandwidth to serve with that capability. Regarding cybersecurity and the advancement of technology, participants viewed U.S. SMBs as being in a challenging uphill battle against hackers.

Participant 1 stressed that "business owners have their head down busy with their companies. They are missing technology trends." In fact, in the context of small and medium businesses, many participants referred to the advancement of technology as "the gap." Participant 4 worried that "I don't know what kind of technology the bad guy will be using but we will be an easy target. Our software is not the latest version and our operating system is unpatched. There is a huge gap between hackers and our company." Similarly, Participant 5 mentioned that "even if our company decides to upgrade their technology today, I'm talking about fundamental IT structure such as computers, hardware and software, it will take a while to catch up to the latest technology." Participant 5 also shared that top management does not seem to have the intention to upgrade the current obsolete systems, despite his multiple requests due to software crashing. Interestingly, all participants revealed that new technology trends are not a noticeable matter at their business organizations, as top management believe and feel that their current cyber structures are adequate to support daily work activities. Participant 1 expressed in a frustrated voice that the skills and knowledge she learned from college and certification can barely apply at her workplace, as the IT infrastructure of the business organization is primitive. Thus, looking at the advancement of technology from the perspective of small and medium businesses, new technology has more negative influence than positive influence. Figure 4 represents the impacts of technology advancement on current information systems in U.S. SMBs. The advancement of technology led to advanced cyberattacks was mentioned eleven times by

participants. In addition, depleting current cyber defense and widening market competition were also the results of technology advancement. Each of this element was mentioned four times by participants.

Figure 4

Impacts of Technology Advancement on Current Information Systems in U.S. SMBs



Theme 3: Lack of Knowledge. Many participants considered lack of knowledge to be the root cause of cyber vulnerability. Participants mentioned this business weakness throughout their interviews, which indicates that the lack of knowledge is the contemporary cyber challenge for U.S. SMBs. According to participants, because many U.S. SMBs are family owned or have "old-school owners," this creates an organizational challenge that weakens cyber-defense capability. In fact, the average age of owners of U.S. small-sized businesses is 50.3 years old, while U.S. medium-sized business owners tend to be a few years older (Experian, 2017). Participants mentioned age as a factor that leads to vulnerabilities in business information systems. Indeed,

Participant 3 mentioned that "[business owner name] insisted on relying on pen and paper because things would be simpler and less complicated" and when Participant 3 brought up cybersecurity, the business owner showed no desire to deal with security challenges. Similarly, Participant 6 mentioned that all of the small businesses she has worked for were conducting business activities as in the past when cybersecurity was not a challenge. All participants stressed that the lack of cybersecurity knowledge is the root causing cyber vulnerabilities, especially social engineering and technical intrusion. Participant 7 pointed out that his company recently bought a firewall "and it is put in the storage room where everyone has access to. I don't know what [business owner's name] is thinking." Nonetheless, Participant 7 still gave credit to his business organization for the effort toward cybersecurity.

Research Question RQ1a Themes. Research question RQ1a was "What are the existing types of barriers that impede enterprises from improving cybersecurity capabilities?" The revealed themes for research question RQ1a not only expose the existing types of barriers that impede enterprises from improving cybersecurity capabilities but also uncover many underlying issues in the field of business. Unexpectedly, responses from participants indicated major disadvantages that SMBs have, comparing to U.S. large companies and corporations. In many ways, these disadvantages directly impact U.S. SMBs in the endeavor to better secure their technology infrastructure in the cyberspace. Specifically, the disadvantages are access to cyber professionals, malfunction of technology system, smaller business scale, financial constraints, and IT workers overwhelmed by being understaffed. With that being said, there were two themes discovered: problems of human resources and the lack of investment in cybersecurity.

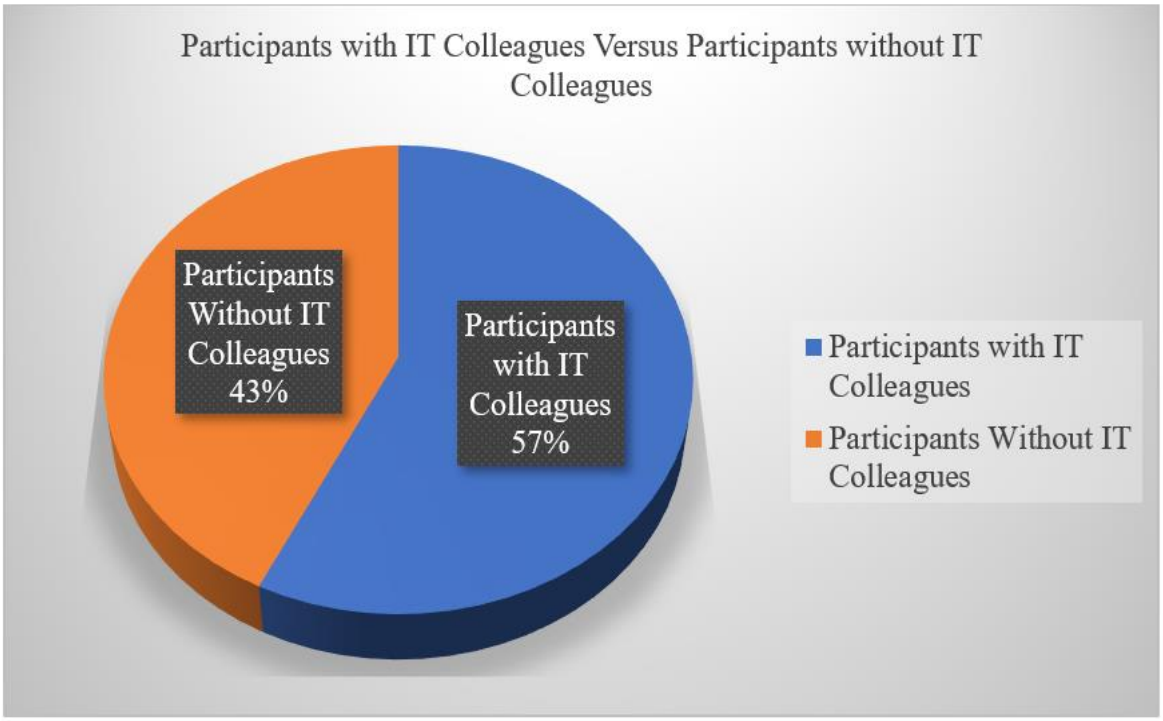
Theme 4: Problems of Human Resources. The demand for cybersecurity jobs is growing rapidly, as in the field of U.S. businesses, the supply of cybersecurity professionals is well below

the demand (Scala et al., 2019). Indeed, the problem of supply shortage of cybersecurity professionals has a significant impact on U.S. businesses as a whole, especially for businesses of small and medium size (Couce-Vieira et al., 2020). The problem of human resources was reflected by angered reactions and unhappy remarks from most participants.

Participant 1 mentioned that she was hired to work in the sole IT position at her business organization. The problem, she noted, is that "I am the only IT person at [company name] and all technology-related issues are put on my shoulder." As a result, the amount of IT support tickets is overwhelming for her, especially IT tickets addressing the malfunction of technology system. "The owner cannot hire another IT support staff with affordable pay rate," said Participant 1. Similarly, because of the old-school business owner, Participant 3 stated that "we still use Windows 7, home routers, and switches. I doubt that the company will hire a cybersecurity guy." Added by Participant 7, SMBs do not have the resources or reputation to approach cyber professionals; therefore, "mom-and-pop business is not always in their list of employers to work for." Importantly, Participant 7 pointed out that, while comparing working for a growing start-up and a mature business, "they got help desk, policy, procedure, boot server. We don't even have Enterprise Edition or a staff with CISSP." Therefore, according to Participant 7, U.S. SMBs will continue to be victimized by cyberattacks because cyber professionals, the essence of security in a technology system, are absent. The theme of the problems of human resources was further highlighted as only four out of seven participants have one or more IT colleagues at their workplace. Thus, having a solid technology support team composed of employees with cybersecurity skills and knowledge is the existing barrier that impedes U.S. SMBs from improving cybersecurity capability as well as daily business operation. Figure 5 represents the percentage of participants with and without IT colleagues.

Figure 5

Percentage of Participants With and Without IT Colleagues



Theme 5: The Lack of Investment in Cybersecurity. An effective cybersecurity system requires investment. In this sense, investment includes a wide range of factors ranging from organizational measures to technology upgrade. Unfortunately, 100% of the participants in this study responded that there is a lack of investment in technology structure, let alone cybersecurity mechanisms. Indeed, regardless of size, U.S. businesses are behind in investment in cybersecurity to counter cyberattacks (Chronopoulos et al., 2018). Participants discussed the lack of cybersecurity investment from both technical and non-technical perspectives as their business is undermanned with obsolete technology. Participant 4 stated, “We are understaffed at [Company Name]. I don’t know how long I and my coworker can handle the extra workload. The problem is we are the only two IT guys providing support to many staffs working off-site with outdated machine.” Participant 4 added that, in his business organization context, making

investment toward upgrading technology will not only decrease his workload and improve business operation but also strengthen the cybersecurity capability of old-age network. Importantly, Participant 2 provided a valuable perspective on the lack of investments in cybersecurity:

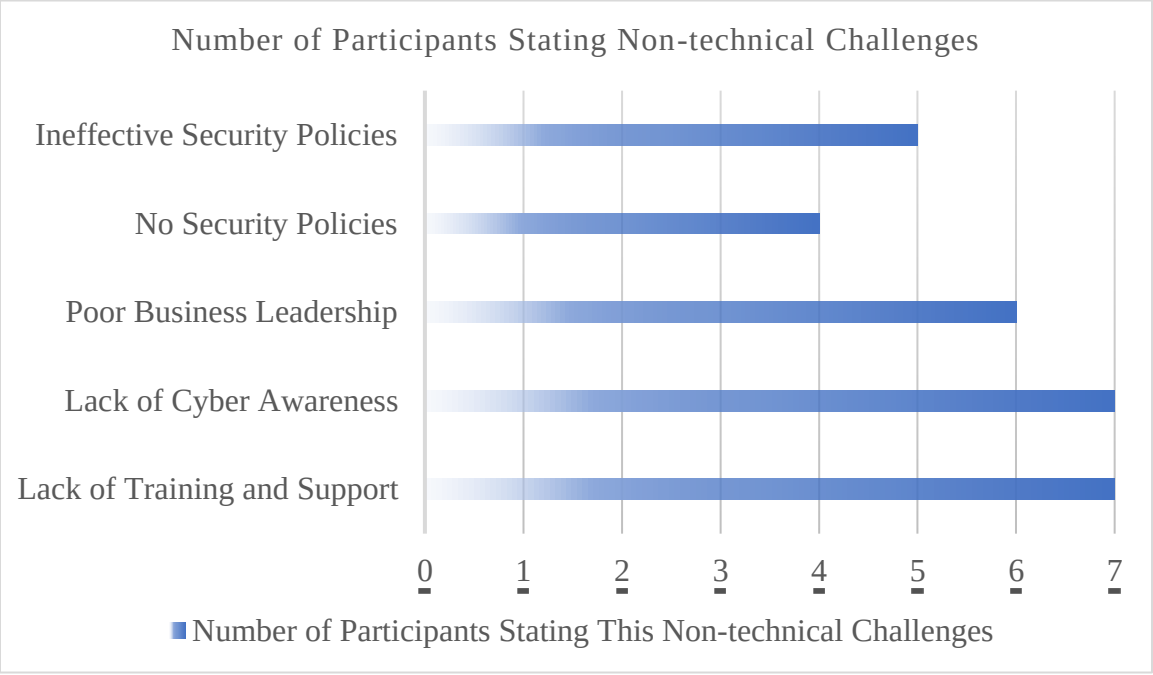
> You put money into cybersecurity. That is not a direct revenue driver . . . A small business looking at where to invest in the organization, their priority for investment is for growth. That is why budgeting and funding go to operation and sale. The criticality of business is to make more money, to hire three or four heads in sale to bring in more revenue. Spending resources on cybersecurity, you know, is not making you money. In the context of small and medium businesses, they are very careful about how to spend money. So, cybersecurity is not in the picture. It's actually viewed as a burden, not an investment! Cybersecurity is culturally growing but it will take years or decades for Tier 1 to be highly secured.

In reality, the solution to the lack of investments in cybersecurity is often not a willing choice from businesses. Particularly, Participant 6 mentioned that a few small businesses that she had worked for were required to upgrade to a certain cybersecurity standard when they signed contracts with cybersecurity-aware corporations. In addition, one of her past employers was a victim of dumpster diving that led to a series of social engineering attacks, resulting in a major investment for a better cyber infrastructure. Therefore, regarding cybersecurity investments, U.S. SMBs view security funding as a burden and only choose to upgrade their cyber capability when they have been attacked or forced to do so.

Research Question RQ1b Themes. Based on participants' responses, organizational barriers were deemed as one of the most forceful factors of creating vulnerabilities in SMBs. Small and medium businesses alike continue to fall for cyber perpetrators, even with advanced technology in business organizations. This is due in part to organizational barriers relating to security capability of SMBs. Specifically, mishaps and lack of awareness, "useless" and "inapplicable" training programs, and ineffective and nonexistent security policies are, as discovered, the current constraints. These constraints wee indicated as a plague in all participants' business organizations. With these elements revealed, the discovered themes were human factor as the weakest link, training and support, and security policies. Figure 6 represents the non-technical challenges for cybersecurity in U.S. SMBs, as stated by participants.

Figure 6

Non-Technical Challenges for Cybersecurity in U.S. SMBs



Theme 6: The Human Factor Is the Weakest Link. Even if businesses are equipped with advanced cybersecurity tools guarding their digital assets, hackers still have ways to prey on the cyber chain of businesses due to psychological flaws. In other words, according to participants, many business processes, from corporations to small enterprises, still require human and manual input, for which exploiting this weakest link remains a fertile target for digital perpetrators. Importantly, as Participants 3 and 5 stated, with business management that does not believe in cybersecurity and with an outdated computer system, a business organization is inviting cybercriminals to take advantage of them. Explaining human error as the most vulnerable cyberattack entry point, Participant 6 discussed in detail the common characteristics of U.S. SMBs in the context of cybersecurity. Participant 6 stated that the human factor will always be the weakest link, which is why scam artists and hackers focus on this link exclusively. Importantly, she stressed that

> it's extremely difficult to protect against that [human factor] because a computer is easy to tell it what to do but sometimes people just act irrational. They go to the wrong site then plug in their credential. Cybersecurity for small and medium businesses is like the wild west! Hardly any foreseeable incoming attacks. Criminals could take a shot to test out businesses, if they succeed in attacking, they succeed, if not, they move to a next one. Sometimes small and medium businesses got victimized from a source that no one could ever think of. It's unimaginable! For example, an employee uses an email that is used for both personal and business to sign up for a website or a service. That service gets hacked and later hackers use the email of that employee to attack the business he works for.

Adding to Participant 6's remark, Participant 5 gave a similar example: "MyFitnessPal, an app everyone has. They had a big breach with emails, even Home Depot was affected through

their employees. Their info got pulled up and falling off to the dark web." Noticeably, Participant 5 pointed out that many SMBs were victimized in MyFitnessPal's cyber incident; however, the media barely addressed the damages. As shown in all participants' responses, human factor, especially mishaps and lack of awareness, will always be the Achilles' heel of any organization.

Theme 7: The Less Training and Support, the More Depleted Cybersecurity Capability.

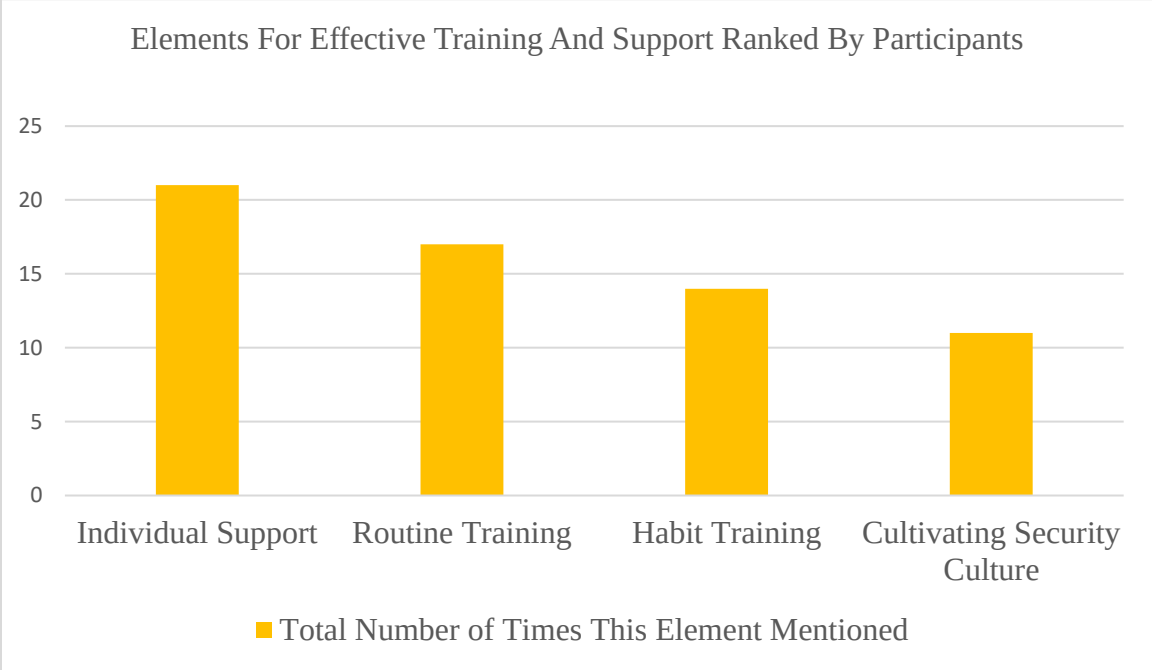
The predominant belief of every participant in this study was that the phrase *cybersecurity capability* is synonymous with four words: human factor, training, and education. According to study participants, one of the biggest organizational barriers for improving cybersecurity capability is training and support. Four participants mentioned that their business organizations do not have cybersecurity training, while three participants acknowledged that the current training programs are "useless" and "inapplicable." Participants viewed the absence of training or ineffective training as an organizational barrier to better cybersecurity, as many SMBs disregard security training. Regarding this matter, Participant 3 revealed that "many companies that I know only have training programs because they are required to by other companies when they sign a business contract. So they quickly create a training program and it is poorly planned." From the perspective of participants, ideally a training program must address not only the danger of different type of cyberattacks but also the expected response for employees. For training to be effective, a training program must be iterated repeatedly for which, according to participants, employees will have security habits and security culture will be imbedded into business organizations. Participants suggested either "quarterly" or "twice a year" training programs. Four participants mentioned the importance of ensuring that new hires receive training to get on board.

In addition to training, a support system is necessary to maintain the effectiveness of training through all levels of a company. Participant 7, a cyber professional with experience working for both corporations and small businesses, suggested that small and medium business organizations need an employee or a team dedicated to supporting other employees regarding training for cybersecurity, such as “providing up-to-date resources” or “offering help individually.” In contrast to Participant 7, Participant 1’s view of support after training program is testing, then improving. “Company can test everyone on different things such as privacy, phishing, data classification, data handling,” suggested Participant 1. She also gave an example that a “company can send fake phishing emails to people in the company and the company can gauge how well the training is, based on how many people clicking on those things.” Importantly, training and support is considered a highly critical measure for minimizing employee-caused cyberattacks, especially social engineering, according to participants. All participants concluded that, based on their observations and experience, the less training and support for cybersecurity a business has, the more attractive they appear to be in the eyes of an intending cyber perpetrator.

Figure 7 represents the elements for effective training and support, as stated by participants.

Figure 7

Elements for Effective Training and Support Ranked by Participants

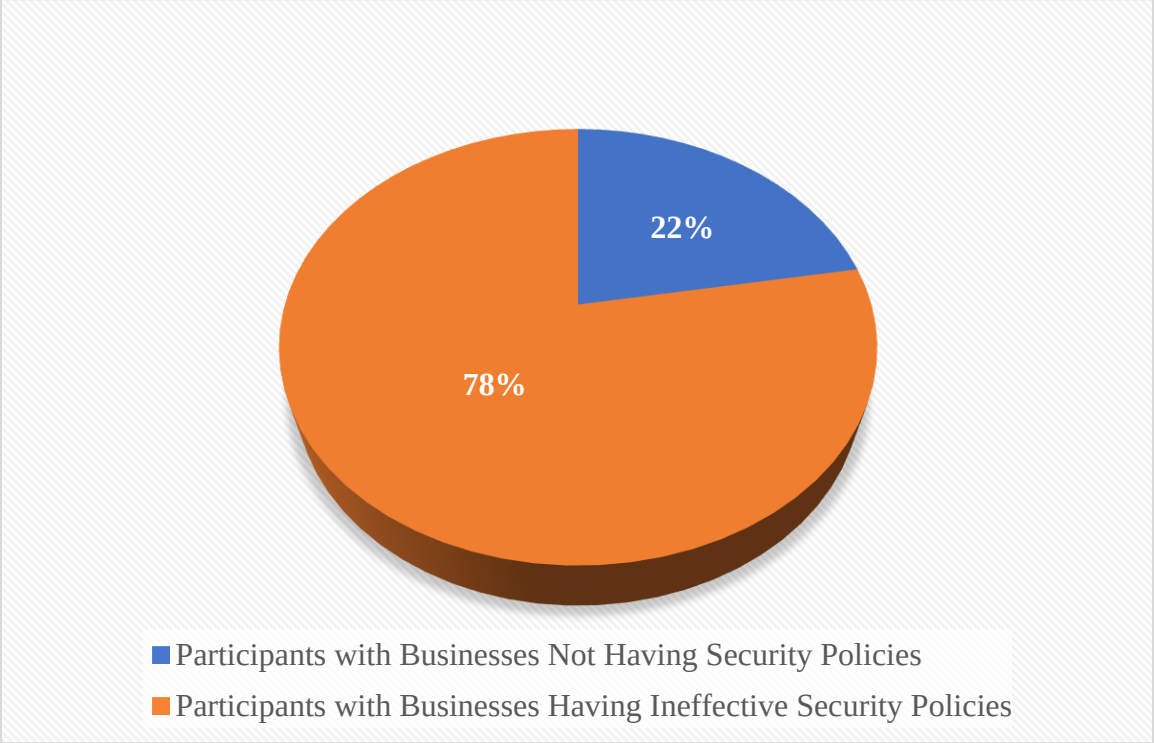


Theme 8: Security Policies. Security policies set the standards of employees' activities in addressing protecting the cyber infrastructure of a business organization. Together with training and support, security policies provide a clear guideline for all stakeholders in a business to follow and uphold to prevent cyber breaches. Nevertheless, all participants mentioned that not many U.S. SMBs have written cybersecurity policies, while some business organizations have vague policies. Therefore, it was a consensus among participants that the matter of security policies is a contemporary organizational obstacle for improving cybersecurity capability. "Most small businesses use off-the-shelf security policies that are from security industry standards. It should only be the baseline because each business is different," noted Participant 4. He also added that an SMB should combine off-the-shelf security policies and policies tailored specifically to human resources and technology infrastructure of that company. Interestingly, most participants mentioned the crucial point that having and enforcing a business-specific

security policy would cost significantly less than the damage from a cyberattack. As Participant 2 put it, “Having a tough security policy is the least any business could do. They don’t have to make any big investment or major change.” In addition, security policies are not only an organizational obstacle regarding cyber defense but also a legal and business-growth matter. Participant 6 noticed that when an SMB grows and becomes a public company, they are legally required to implement cybersecurity policies in many regulated industries. Besides the type of industry, she also noted that some states require a baseline security policy to conduct business activities in their states. This point leads to the premise that without a security policy or with only a vague one, U.S. SMBs are barred from growing. From participants’ perspectives, implementing an effective security policy is currently an organizational challenge for better cyber defense because a security policy not only defends against social engineering cyberattacks but also serves as a layer in the multilayered cyber defense of any business organization. Figure 8 represents the percentage of participants with businesses having security policies, as well as those whose businesses lack security policies.

Figure 8

Percentage of Participants With Businesses Having Security Policies



Subtheme: Awareness: Participants Discuss Security Awareness Through Two Approaches: Training and Policy. Responses from participants indicated that, with security policies, employees feel obligated to conduct business activities with security standards in mind. Participants 3, 5, and 6 stated that business can address awareness on many different levels, from all staff members to management level and to specific job roles. In addition, most participants believed that awareness through security policies should be constantly reminded through different channels of communication. Participant 2 gave an example that "sometimes you can put out a little helpful hint like a sign reminding everyone has to badge in to get through the door, one person at a time! or having security reminders on the company asset such as report suspicious spam or attachment to . . ." Because a cyberattack involves both technical and

organizational elements, participants believe that improving awareness through security policies somewhat helps minimize the risk or the damage of an attack.

Research Question RQ1c Themes. Research Question RQ1c was "How impactful are technical barriers on small and medium enterprises in improving their cybersecurity capability?" When asked about how impactful technical barriers are on U.S. SMBs, all of the participants' responses focused exclusively on the obsolete technological infrastructure that they have experienced within their small- and medium-sized enterprises. Importantly, the challenges originating from obsolete technological technology were discussed in depth by participants because of the belief that, from a technical standpoint, cybersecurity capability is significantly constrained by using outdated technology. It is a consensus that the level of technological sophistication in today's perpetrators outmatches many businesses' information technology and cybersecurity mechanisms, due to a variety of both technical and organizational weaknesses. As shown in all of the interviews, obsolete technological infrastructure is the most concerning technical barrier, which leads to other cyber risks in U.S. SMBs. According to participants, these cyber risks are the incapability of preventing popular cyberattack methods and the inability to prevent cyberattacks originating from employees' mishaps. In addition, based on participants' responses, financial resources and underinvestment is a lethal limitation affecting the current state of technological infrastructure.

Theme 9: Obsolete Technological Infrastructure. All participants reported the state of their companies' technological infrastructure as ranging from somewhat outdated to significantly obsolete. An obsolete technological infrastructure is an extreme threat for any organization, ranging from cybersecurity to business operation and continuity. Participants expressed their disappointment in the outdated computers and systems. Based on participants' responses, the

definition of obsolete technological systems is software that ceases to be updated and is incompatible with other software and hardware, or hardware that reaches age limits. In other words, the obsolete technological systems are where the vendor no longer supports the software and hardware or provides maintenance. Participant 4 expressed concern that "the more outdated the company's software is, the more vulnerable we are in the eyes of hackers." He also stated that patching and updating are not a long-term solution for both cyber defense and business process. Sharing a similar perspective, Participant 7 mentioned that "business cannot keep patching their software. It may be a quick-fix but patching adds more layers of complexity that create recovery and redundancy issues." Regarding outdated hardware, participants believed that hardware generally has longer lifespans than software. Therefore, in terms of hardware, businesses do not need to replace them before a certain time. Noticeably, as Participant 7 stated, "Businesses can replace a majority of their hardware every five years and the replacement won't severely affect their budget if they focus on the right items." However, according to Participant 7, it requires technical knowledge to strategically implement new hardware, which is a significant limit for SMBs. Besides risks and threats from cybersecurity, participants viewed that changes in business practices and processes render their companies' systems outdated. Importantly, five out of seven participants acknowledged that if their organizations acquired and implemented up-to-date systems, they would have reached more potential customers, not only the current limited pool of customers.

Subtheme: Financial Constraints. From the perspectives of all participants, financial resources are a major problem for U.S. SMBs in terms of investing in defending their organizations on the cyberspace. Limited budgets already pose many challenges for small and medium enterprises; therefore, according to participants, upgrading cyber-defense capability

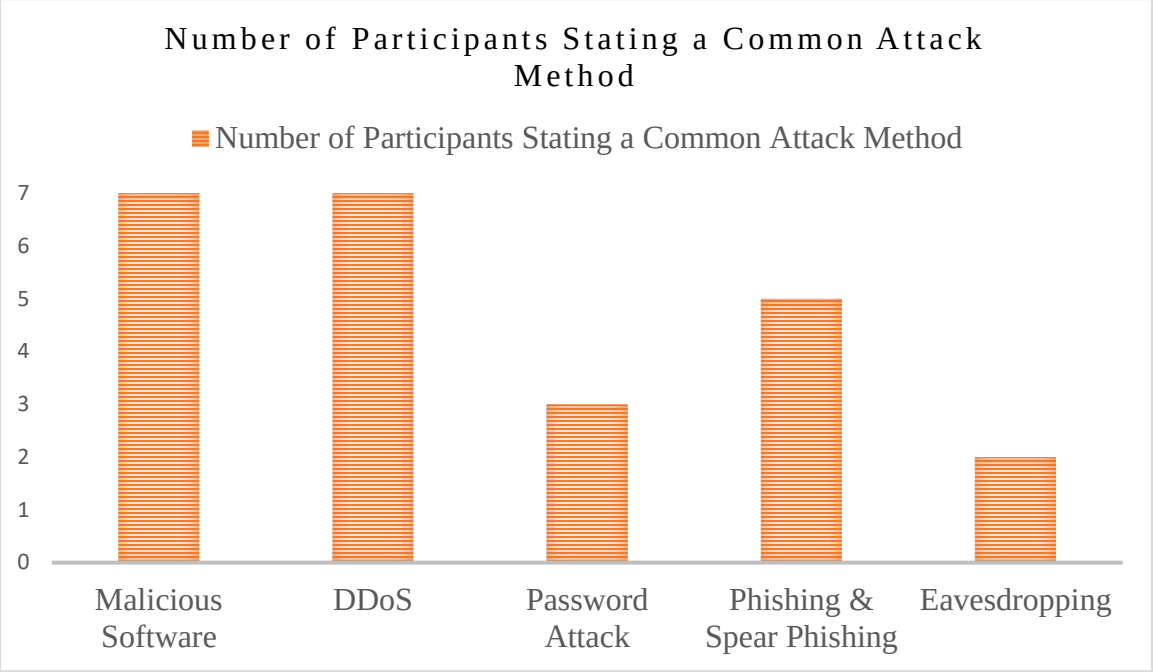
from an outdated technology system is not the priority. As Participant 2 viewed, spending for cyber defense is a “burden,” rather than an investment. This philosophy was reinforced by other participants as Participant 5 stated that “small businesses do not have the money for a cyber defense system that can fight off common cyberattacks. If they decide to upgrade their technology, it will take years because companies don’t have the budgets for one-time upgrades, and they are already behind in the game.” Adding to this point, Participant 3 remarked, “Businesses tend to sweat their technology assets as long as possible to save costs. That’s why even if their computer system is outdated but usable, they are not willing to upgrade.” More succinctly, Participants 3, 4, and 6 revealed that because of the limited financial resources in conjunction with the lack of cyber knowledge, U.S. SMBs often base their decisions more on price than on cyber functionality, especially those businesses with older business owners and decision makers. As a result, participants believe that financial constraints pose a highly complex barrier for U.S. SMBs. This complex barrier prevents U.S. SMBs from solving the challenges of the current obsolete technological infrastructure impacting cybersecurity capability.

Subtheme: Existing Technology Is Incapable of Preventing Popular Cyberattack Methods. In the context of obsolete technological infrastructure, participants believe that the current technology in U.S. SMBs is vulnerable to common cyberattack methods that could have been prevented with a basic upgrade. Participants discussed a wide range of attack methods that U.S. corporations with better technology are immune to; however, these attack methods remain a problem for SMBs. The common attack methods that were mentioned and discussed in depth are malicious software, DDoS, password attack, phishing and spear phishing, and eavesdropping. Noticeably, perpetrators relying on phishing emails with attached malicious software are the major concern, as employees are not well aware of fraudulent communication and the obsolete

computer systems are incapable of defending against malicious code. All participants noticed that the discussed cyberattack methods are a combination between social engineering and technical procedures. More specifically, participants mentioned how a company can be divided into different sensitivity levels of employees to prevent the attack happening or to mitigate the damages. Participant 7 mentioned in depth that "companies can reengineer their network assets based on the concept of security segmentation that uses firewalls separating employees, so attacks are stopped right at the contact point." Adding to this recommendation, Participants 2 and 5 advocated for the use of active directory, as this directory service is included in most Windows domain networks in new Windows Server operating systems. According to some participants, the choice of a method such as screened subnet, hardware, or active directory tree depends on the current state and capability of the existing technological infrastructure of each business. Nevertheless, the fundamental factor that was primarily discussed is that the current obsolete technological infrastructure requires the massive financial resource for U.S. SMBs to upgrade for a solid cyber-defense capability. Figure 9 depicts the common attack methods addressed by participants. Malicious software, DDoS, password attack, phishing and spear phishing, and eavesdropping were the significant concern for U.S SMBs.

Figure 9

Common Attack Methods Addressed by Participants



Subtheme: Existing Technology Should Be Able to Prevent Cyberattacks Originated From Employees' Mishap. From the viewpoints of participants, when employees fail to follow cybersecurity rules and guidelines or compromise the network infrastructure, the technological infrastructure should function as a safety net that prevents or controls cyber damages. Nevertheless, all participants asserted that the primitive technology of U.S. SMBs does not have that level of assurance. Responses from participants indicated the alarming vulnerabilities of network infrastructure in small and medium companies. Four participants gave firsthand account examples of how a mistake of an employee or a business partner resulted in a cyber breach, from which financial data and business information were leaked. They believed that with better technical support and design, the risks would have been stopped before they became damages. Furthermore, comparing the state of technology infrastructure between SMBs and corporations,

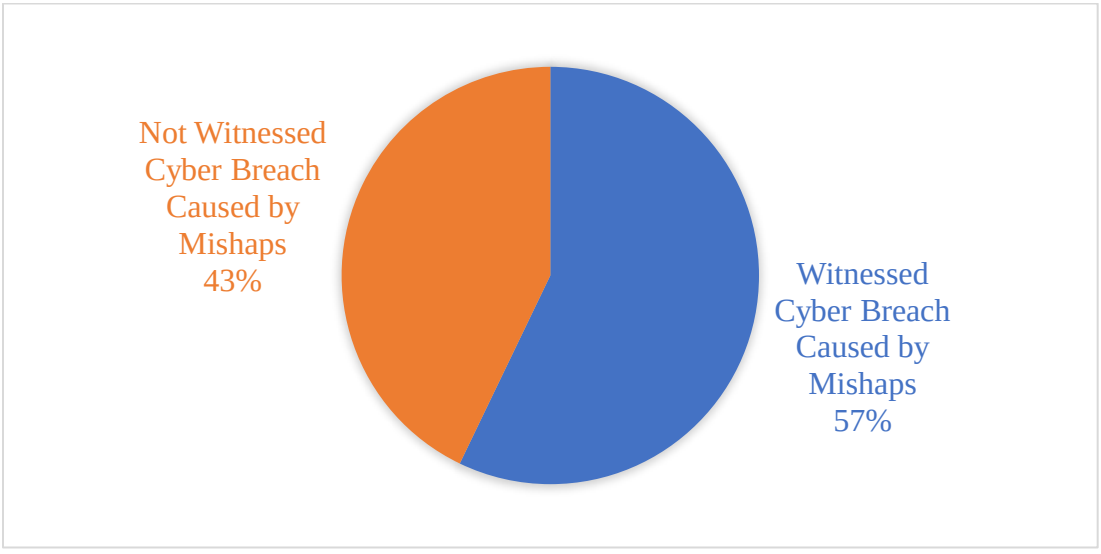
Participant 7, a cyber professional with experience working for a Fortune 500 company and an expanding medium business, was most concerned.

> At most US corporation, if an employee makes a mistake on the network, it doesn't affect everyone else. The threat is likely isolated in a function. Because their infrastructure comes with separation in data center, entirely different hardware, different access control. This is the luxury big businesses have that most small and medium businesses don't. The key distinction is the level of technology.

More importantly, this participant also pointed out that even with state-of-the-art cyber-defense mechanisms, U.S. corporations still make headlines as cyber victims; therefore, the day when current SMBs with old technology become highly secured against major cyber threats is still decades away. This pessimistic viewpoint was also shared by other participants. Figure 10 represents the percentage of participants who have witnessed employees' mishaps resulting in cyber breaches.

Figure 10

Percentage of Participants Who Have Witnessed Employees' Mishaps Resulting in Cyber Breaches



Research Question RQ1d Themes. Research Question RQ1d was "What are the practical cybersecurity mechanisms that could boost the cyber-defense capabilities of small- and medium-sized businesses?" When asked questions related to applicable technical mechanisms that U.S. small and medium businesses could utilize to limit the occurrence and intensity of cyberattacks, participants emphasized security for the new trend of business technology and seeking the cyber solution from outside of the organization. From participants' remarks, two themes were attained. They are outsourcing cybersecurity and bring-your-own devices. While these two approaches were believed to be the applicable technical mechanisms that business organizations need to implement instantaneously, they require some organizational elements to attain these technical mechanisms. In other words, for the success of any technical mechanisms' implementation, organizational support and rational business decisions are the vital foundation. Table 2 represents the applicable technical mechanisms for U.S. SMBs, as mentioned by participants.

Table 2

Applicable Technical Mechanisms for U.S. Small and Medium Businesses

Applicable Technical Mechanisms for U.S. SMBS	Number of Participants Mentioning This Approach	Total Number of Times This Approach Was Mentioned
3rd Party Cybersecurity	6	21
Commercial Off-the-Shelf Products	7	24

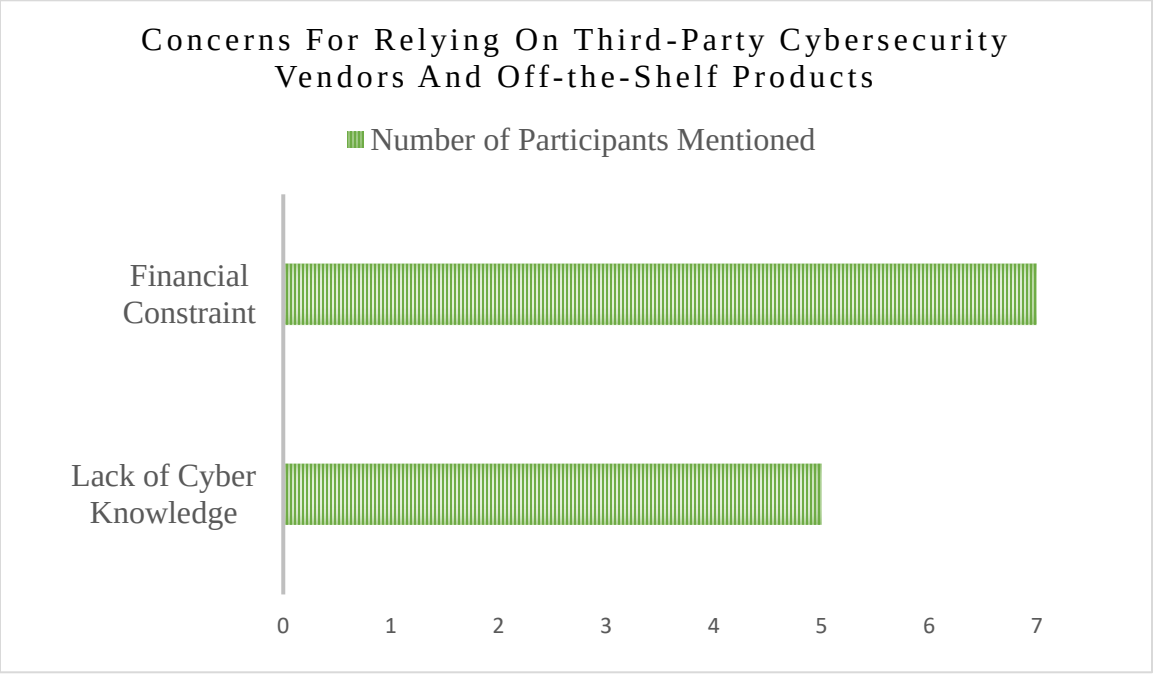
Theme 10: Outsourcing Cybersecurity. Participants favorably recommend that U.S. SMBs outsource their cybersecurity to a third party for many reasons. Two major grounds for outsourcing to one or more third-party cybersecurity vendors are cost savings. This can be accomplished by eliminating on-site security team or personnel when choosing appropriate vendors, and better cyber assurance. Regarding cutting security expenses by choosing appropriate security vendors, many participants believe that U.S. SMBs would eliminate major on-site hardware, software, and personnel. Participant 5 gave an example that "a company wants [to] get rid of their outdated mail server in the basement and the IT guy who maintains it. They can migrate to the cloud and I hope they choose O365 with many security attributes." Currently, according to participants, the majority of U.S. SMBs use off-the-shelf products that somewhat support their business activities; however, their security competence is less than decent. Addressing this point, five participants considered the selection of highly specific products and services that not only provide support for business operation but also come with built-in cybersecurity characters. To sum up this point, Participant 2 confirmed that "the bottom line is companies aren't inherently buying security tools but buying products for solution that are . . . have security tools built into them." More importantly, participants believe that this business decision raises a major challenge for which, as Participant 2 put it, a "company cannot just Google and find a third-party security company. It takes a lot of time to research what's suitable and what's not." Responses from participants indicated that the lack of knowledge is a major barrier for outsourcing cybersecurity to one or more third-party vendors.

Regarding better cyber assurance by outsourcing cybersecurity, participants believed that third-party vendors evaluate the cyber situation and update proactively based on the more current cyber-risk situation in the field, as compared to U.S. SMBs having an on-site dedicated

cybersecurity team. In addition, most third-party cybersecurity vendors offer solutions based on need assessment, for which services are tailored to the nature and requirement of each SMB. The majority of participants advocated for the advantages of cyber assurance from third-party vendors, as this strategy would bring "new set of eyes," "frequent internal and external scanning," and "identifying things that others may have not found." Moreover, while advocating for outsourcing cybersecurity, all participants expressed major concern about business expenses as U.S. SMBs have a tight budget for most of their business objectives. To sum up from participants' responses, the underlying key factors for the successful outsourcing of cybersecurity to vendors are budget, business solutions with imbedded cybersecurity, and effective strategic decisions. U.S. SMBs must do their due diligence to balance the cost and the benefits of choosing the outsourcing cybersecurity route. Figure 11 represents participants' concerns regarding relying on third-party cybersecurity vendors and off-the-shelf products.

Figure 11

Concerns for Relying on Third-Party Cybersecurity Vendors and Off-the-Shelf Products



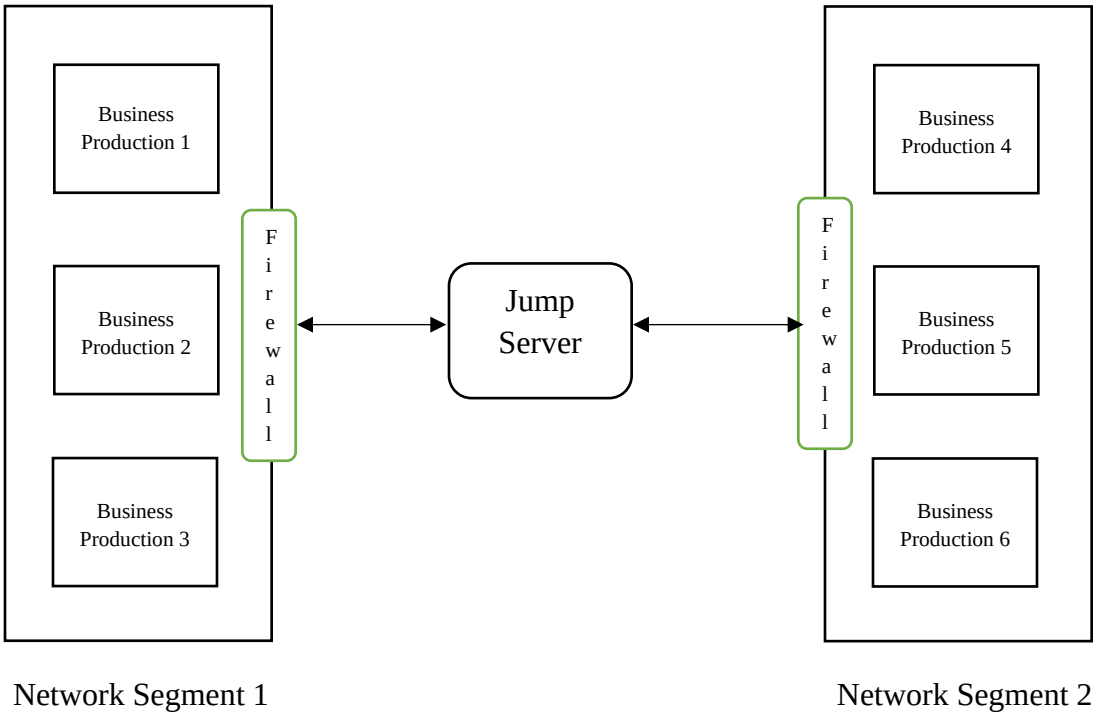
Theme 11: Bring-Your-Own Devices: Policy and Network Segmentation. In the beginning, using personal devices for business-related activities was encouraged**,** as the use of these devices saved time for employees while cutting down costs of businesses (Chang et al., 2014; Miller et al., 2012). Nevertheless, using personal devices for business activities, also known as bring-your-own device (BYOD), caused enormous cyber risks**,** for which even well-known Fortune 500 corporations were victimized (Chang et al., 2014; Miller et al., 2012). As a result, U.S**.** SMBs are not exempt from being exposed to cyber risks of employees using BYODs. In dealing with risks from BYODs, the first responses from participants were to adopt and implement tough policies on personal devices connected to the company's network. Based on participants' remarks, BYOD policies must address scope and procedure cautiously**,** based on the technical framework and organizational structure of a business. Participants addressed **s**ome frequently mentioned procedure**s** in BYOD policies, including "restrictions on authorized devices**,**" "technical validation," "boundary of company access**,**" and "device protocols**.**" In addition, five out of seven participants discussed how violations of BYOD policy should be enforced through "disciplinary action" or "termination of employment." In fact, to prepare for the unfortunate outcome, technical and organizational measures must be defined and performed to limit and mitigate cyberattacks once a BYOD is stolen, lost, hacked, or damaged. Participant 7 advocated for the installation of "remote wipe" software, so that employees can remotely "bleach" sensitive company data for which the device's application and both personal and company data are completely destroyed.

Additionally, some participants meticulously discussed the ideal design of network infrastructure for better cyber protection in U.S. SMBs. According to some participants, the concepts of physical and virtual segmentation are highly effective in separating BYODs and the

company's network asset. By doing so, any cyberattack against one or a group of BYODs would be isolated and mitigated, as a cyber threat cannot move freely through the entire network system. While five participants verbally discussed the concept of segmentation, Participant 5 illustrated this concept with a sketch of the network design, shown in Figure 12.

Figure 12

Network Segmentation for Bring-Your-Own Devices



According to participants who discussed the concept related to Participant 5's visual illustration, BYODs in each business production in this network design are contained in an individual production environment. "There's nothing you can do with your mobile device that can compromise the other production environment and where the product actually lives. They are two totally separate things," according to Participant 5. While drawing out the above illustration,

Participant 5 stated that the smaller an organization is, the less complications and components of security segmentation for that business entity to implement. To sum up, according to most participants, the technical soul for a secured network with BYODs is access control. This point is critical as U.S. large businesses and corporations have more technical capability in controlling BYODs from the user end, while U.S. SMBs are limited at the access point of their technical infrastructure.

Research Question RQ1e Themes. Research Question RQ1e was "What are the practical organizational mechanisms that could boost the cyber-defense capabilities of small- and medium-sized businesses?" When asked questions related to the practical organizational mechanisms for a better defense capability, participants emphasized the internal and external environment of a business organization. Two distinct themes were derived based on their responses. They are conducting evaluation on risks from third party and cultivating an organizational culture for cybersecurity. These two themes are found closely connected to other revealed themes addressing the impactful factors leading to an increasing number of U.S. SMBs falling prey to cyberattacks. Notably, participants believe that business organizations are the defense mechanism in fighting risks from third parties, even before a cyberattack happens. Similarly, cultivating and maintaining an organizational culture for cybersecurity is revealed as essential for limiting security risks, especially those risks that cause social engineering types of attacks.

Theme 12: Conducting Evaluation on Risks From Third Party. The state of cybersecurity in U.S. SMBs has already been vulnerable. Therefore, according to responses, besides internal risks, the risks from third party are highly perilous to the level that could bankrupt small and medium businesses. In the context of the conducted interviews, third parties

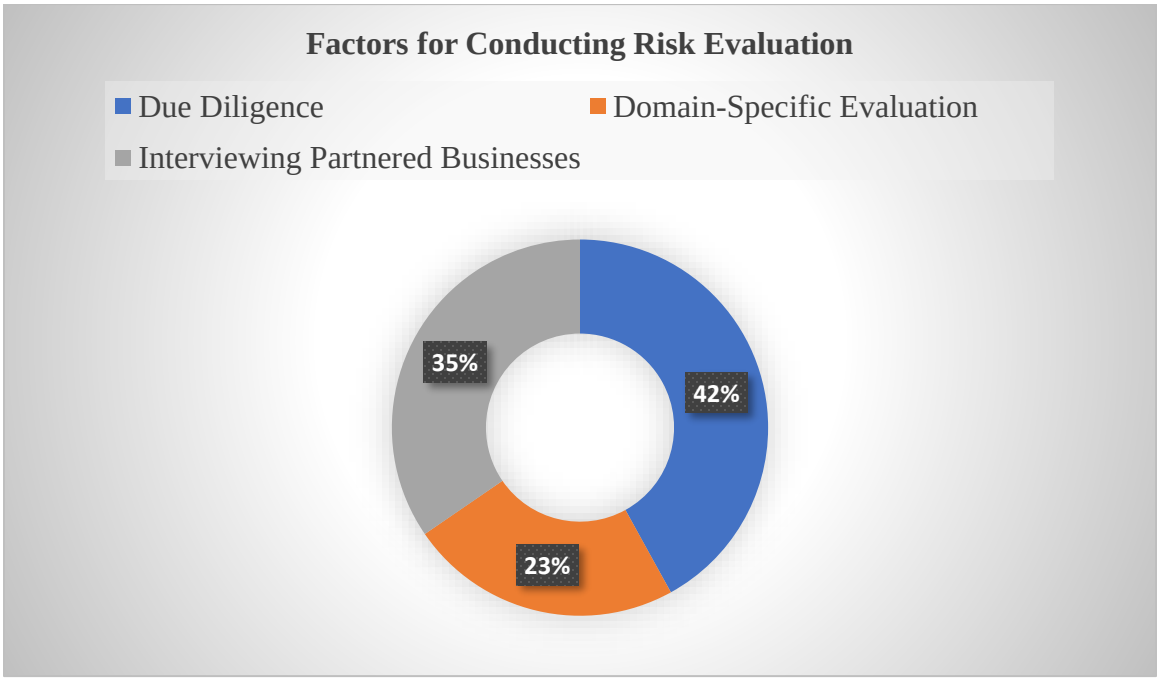
is uniformly defined by participants as business partners or cybersecurity services. Interestingly, most participants discussed risks from third parties with the rationale that many corporations have already been falling prey to cybercriminals multiple times through risks from third parties, with “Home Depot” as the most cited example. Therefore, from participants’ pessimistic points of view, U.S. SMBs have no chance in fighting against third-party risks. All participants affirmed that U.S. SMBs have already been under attack for a long time; however, the aftermath of cyberattacks against these organizations is often unheeded. According to participants, risks from third parties pose unsolvable challenges, as business organizations, no matter the size, do not have the access to fully regulate and deter cyber risks in the technical and organizational systems of their business partners and cybersecurity service providers. Most participants indicated that the applicable approach to address risks from third parties is for SMBs to try their best to defend themselves internally. Noticeably, participants expressed that this solution does not solve the dire cyber situation; however, it is better to be defending proactively than reactively.

Furthermore, Participant 2 ascertained a point that was resonant with all of the participants: “Anytime a company has business partners, third-party risk is always a threat to that company. The only remedy I can think of is to perform evaluation on those companies.” Similarly, Participant 5 highlighted the words “due diligent” when a small or medium business chooses a cybersecurity service or screens a business partner. According to Participant 5, “due diligent” means that a small or medium company conducts a thorough interview of its partnered businesses or a cybersecurity service to find out how they protect their digital assets in the cyberspace. Participant 5 believed that this strategy is more cost effective than sending a company’s cyber professional or hiring a cyber professional to conduct an on-site analysis of the

partnered businesses, as U.S. SMBs do not have the technical and financial capability to do so. Participant 4 added to Participant 5's suggestion that as not many businesses allow cyber professionals from other businesses to conduct cybersecurity analysis on their critical infrastructure, acquiring as much information as possible about cyber-defense capability from business partners is more sensible. Noticeably, Participant 4 summed up the main concern of other participants that a business should "take what other businesses claim about cybersecurity at their organizations with a pinch of salt" while persistently pursuing the most practical strategy combating against third-party risks, which is to toughen up on specific security domains to which partnered businesses could pose a risk. Figure 13 represents factors for conducting evaluations on risks from third parties and the percentage of participants who mentioned each factor.

Figure 13

Factors for Conducting Evaluation on Risks From Third Parties



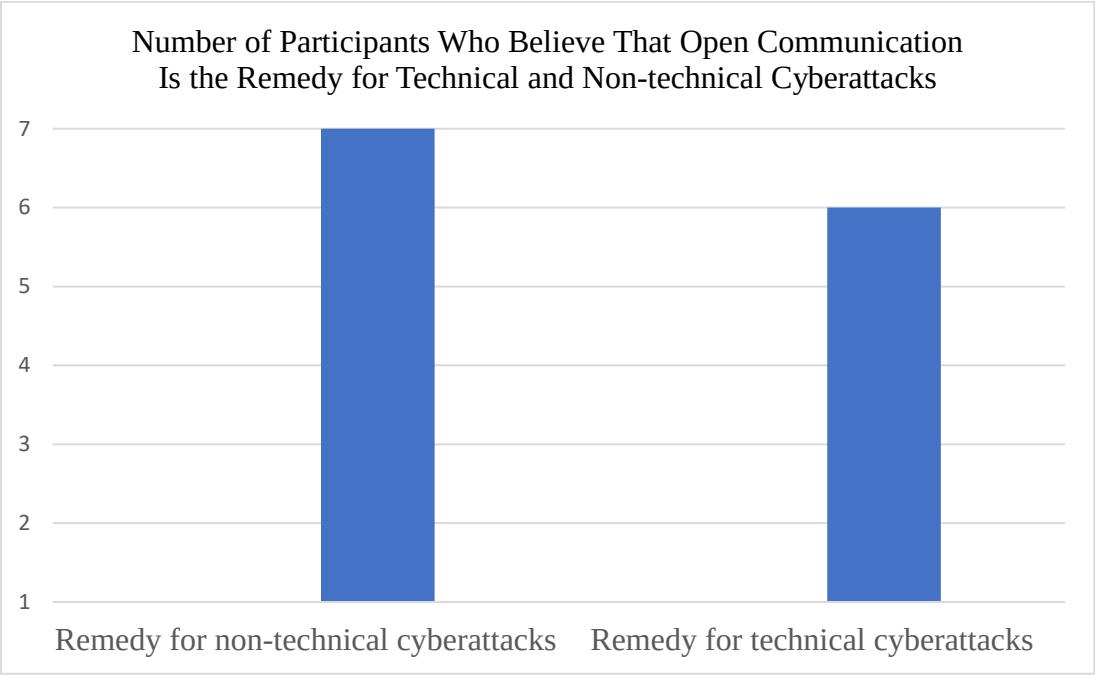
Theme 13: Cultivating an Organizational Culture for Cybersecurity. The theme of cybersecurity cultivation is interconnected to other themes, as advancing a culture of

cybersecurity is the common belief among participants, who noted that behaviors of employees have major impacts on cyber defense. Therefore, cultivating an organizational culture for cybersecurity was touched upon by participants. Participants believed that implementing and emphasizing a culture of cybersecurity would limit security risks and social engineering attacks. To cultivate an organizational culture for stronger cybersecurity, there are two strategic points that participants discussed exclusively. Those points are open communication and formulating and maintaining strategic relationships between employees, especially between IS professionals and other employees.

To accomplish the development of a strong cybersecurity culture, open communication among stakeholders of an organization is deemed significant. Participant 5 viewed a lack of communication that "leads to miscommunication" as the greatest risk for building a culture of cybersecurity and awareness. Participant 2 considered clear, open, and thorough communication between employees as "the most important thing." He gave an example that "everyone in a company should feel comfortable asking questions. If my coworker receives an email with attachments from me, he should feel comfortable and encourage to call in and say 'Did you send this?'" Furthermore, participants strongly believe that any organization with a culture allowing open communication without chastisement enables itself to defend against social engineering attacks naturally. Thus, open communication is considered the non-technical remedy for fighting against both technical and non-technical cyberattacks. Figure 14 represents the participants' beliefs that open communication is the remedy for technical and non-technical cyberattacks.

Figure 14

Participants' Beliefs That Open Communication Is the Remedy for Technical and Non-Technical Cyberattacks



Maintaining strategic relationships among employees, especially between IS professionals and non-technical employees, cultivates an organization's cybersecurity culture through building a strong human resource network focusing on cyber defense. For a strong human resource network of cyber defense, participants indicated that the strategic relationships between IS professionals and other employees "will get everybody in the company [get] on board." In Participant 1's words, IS professionals will "lead the culture change." Based on remarks from participants, the functions of IS professionals in building a security culture are accomplished through relationship; cyber professionals eliminate resistance to change, provide resources and support for cyber defense, and lead everyone toward cyber goals. Thus, formulating strategic relationships between employees, especially between IS professionals and

non-technical employees, is essential for a security culture, as everyone in an organization is actively involved in defending against cyberattacks.

Relationship to the Conceptual Framework

The findings in this study are found consistent with the conceptual framework presented in Section 1: Foundation of the Study. There are three fundamental parts of the conceptual framework. They are cyber situational awareness theory, cyber defense mechanisms theory, and Control Objectives for Information and Related Technology (COBIT) 5. Succinctly, responses from participants are aligned with all components of the three fundamental parts of the conceptual framework. These components cover the human aspects of cyber defense, the technical aspects of cyber defense, and cyber defense capability.

Cyber Situational Awareness (CSA) Theory. Cyber situational awareness theory focuses exclusively on human aspects of cyber defense (Franke & Brynielsson, 2014; Pöyhönen et al., 2019). This theory also concerns with the organizational decision-making process in private entities (Franke & Brynielsson, 2014). When considering CSA theory in light of the responses collected from participants, significant emphasis was placed on the lack of cyber knowledge, human error triggering cyberattacks, irrelevant organizational decisions and cyber human resources. The theory addresses the non-technical aspects of risk causation of cyberattacks, for which it successfully presents the three human-related challenges and barriers for the improvements of a strong cyber-defense capability. Specifically, the collected responses revealed absences and weaknesses for improving human-related factors in cyber defense of U.S. SMBs addressed in CSA theory. These factors, considered as absences and weaknesses by participants and discussed in CSA, are detection needs for strategic, operational, and technical decision-making levels; situation awareness; and analysis and assessment for impact on future

(Pöyhönen et al., 2019). More importantly, this theory seems to assume that by securing human-related factors in cyber defense, business organizations will achieve close to 100% success in combating cyberattacks (Franke & Brynielsson, 2014; Kemper, 2019; Pöyhönen et al., 2019).

Cyber Defense Mechanisms (CDM) Theory. The findings support the conceptual framework of CDM. Fundamentally, this framework set forth a strategy for business to discourage cyber perpetrators by toughing up defensive mechanisms (Ryan, 2018). While revealing current weaknesses and vulnerabilities of the cyber-defense system in U.S. SMBs, participants align their views with CDM through discussions and recommendations of upgrading the obsolete infrastructure, securing Internet of Things (IoT) devices, implementing cyber deterrence hardware and software, partitioning network, and eliminating data breach through technical procedures. Importantly, there are foundational relations between the findings and the CDM theory. Specifically, technical elements addressed in the findings fit into the two spheres of business's defensive mechanisms. The two spheres are passive and proactive mechanisms. In conclusion, both collected data and CDM theory support a strategy of cyber deterrence: denial-of-attacks strategy for which the plan is to have a powerful defense that cyber perpetrators do not bother to attack.

Control Objectives for Information and Related Technology (COBIT) 5. COBIT 5 has five different domains that cover all elements related to technology in enterprises. The utmost goal of COBIT 5 framework is for decision makers in businesses to enhance control environment, internal control system, and risk assessment (Rubino et al., 2017). In analyzing the relations between COBIT 5 and collected data, it is found that four out of five domains of COBIT 5 were directly addressed in the data collection and that the objectives of this framework, which are control environment, internal control system, and risk assessment, are aligned with the

responses from participants. Specifically, discovered themes have strong relations to four out of five principles of COBIT 5. These four principles are meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, and enabling a holistic approach. Notably, some elements of the fifth principle, separating governance from management, are found consistent with the data collection. These elements are prioritizing decisions and complying with stakeholders' needs based on the organization's capability.

Relationship of the Findings to Research Questions

This case study was designed to reveal the contemporary barriers and challenges impacting cybersecurity competencies of U.S. SMBs. This research study relied on the perception and experience of participants in small and medium business organizations regarding cyber defense as a business risk. Real-world experiences and perspectives of participants were captured and presented, rather than the interpretations of the researcher. This section discusses how the findings relate to the 6 research questions posed in this study. These research questions address multiple angles of the problem of the ever-increasing cyberattacks against U.S. SMBs.

Analysis of Research Question RQ1 Findings. The results of RQ1 were integrated into the overall framework of the problem of the ever-increasing cyberattacks against U.S. SMBs. The three themes, technology deficiencies, advancement of technology, and lack of knowledge, exposed the alarming weaknesses that SMBs are extremely vulnerable in crucial areas. These areas are divided into two spheres: technical and non-technical. The technical areas are deficiencies in software and hardware, technical burden for IT professionals to fulfill job functions, and insufficient business process due to deficient technology. The non-technical aspects of cyber weaknesses for RQ1 are a disregard of cybersecurity from top management, the impact of age factors on technology, irrational decision makers, and the lack of support from

leadership to working cyber professionals. Based on responses from participants, revealed information indicates that U.S. SMBs are not only having technological obstacles for a better cyber defense but also a cyber workforce that feels unsupported and overlooked. This finding entails why U.S. SMBs are continually becoming prey of cybercriminals.

Implications of Research Question RQ1 Findings. U.S. SMBs benefit from these findings by being alarmed regarding how business organizations become easy targets for cybercriminals. The finding provides guidance for U.S. small and medium business on specific areas in which to initiate a comprehensive assessment. This assessment is to address the combination of their state of technology and workplace environment. Because each business organization is different, each assessment result will indicate which areas are the top priority for that business to reform. In terms of the state of technology, there are indications that the new upgraded technology should not only strengthen and reinforce cyber-defense capability but also improve and enhance business process. Importantly, workplace environment, for which feedback from participants was unsupported from management and burdened by technology, must be reformed with both technical solutions and better leadership approach. Altogether, the challenges and barriers for a stronger cybersecurity, which have been previously presented, will be subdued.

Analysis of Research Question RQ1a Findings. The combined Themes 4 and 5, problems of human resources and the lack of investment in cybersecurity, flow together to form the core hardship of U.S. SMBs in the race against cyberattacks. The findings of two themes reveal the underlying problems that a majority of small and medium businesses encounter. Feelings about the challenges from the demand for cyber human resources and security investments are frustrated, abandoned, hopeless, and disappointed from employees. Most often, when discussing cybersecurity, the focus is usually the technical and non-technical mechanisms

and solutions to combat attacks. Significantly, the findings reveal the dire state resources and support for those mechanisms and solutions. While Themes 4 and 5 were collected and generated in the context of cyberattacks against businesses, the real-world problem they expose are U.S. SMBs having dilemma with acquiring enough cyber talents, obtaining sufficient financial source, and allocating appropriate investment in specific areas of organizational defense. Significantly, RQ1a addresses background factors that go beyond the common concerns of cybersecurity in businesses, which often are cyberattacks and cyber defense.

Implications of Research Question RQ1a Findings. The findings shed light on the obstacles that U.S. SMBs must resolve, which are cyber talents, financial source, and appropriate investment in specific areas of organizational defense. These obstacles are, in fact, the fundamentalities for fortifying the almost non-existent cyber-defense system in business organizations. In reality, it will take a long time for U.S. SMBs to overcome the obstacles generated from the lack of cyber talents, financial source, and appropriate investment to needed areas of cyber defense, due to their organizational nature. The organizational nature implied by participants is that these business organizations are often family owned, with limited scale in the vast market. They are not only competing against cyber perpetrators but also larger business entities in terms of attaining cyber talents and financial source. These findings imply the suggestions that U.S. SMBs must be successful in securing large financial source to hire more cyber talents and to invest in vulnerable cyber-defense areas in their organizations.

Analysis of Research Question RQ1b Findings. No matter how advanced the cyber defense system is, U.S. SMBs will always be victimized by cyberattacks if human-related issues are not resolved. That is the conclusion of the findings generated from the responses of participants. The human-related issues revealed are employee mishaps and errors, lack of

training, the lack of security policies and their enforcement, and the lack of cybersecurity awareness from employees. From this analysis point of view, these issues are not only the non-technical elements of cyber defense but also organizational barriers for cybersecurity capability in small and medium enterprises. These findings point out that all stakeholders in a business, from top of the organization to the bottom, are a piece of the puzzle in the complete picture of cyber defense of an entity. When an employee is reckless, no matter what their position in the organizational ladder, a cyber catastrophe ruining the primitive technical infrastructure of small and medium business will always be the consequence. Importantly, the findings indicate the pessimistic view that human issues are nearly impossible to solve because a small error could undermine the entire system or effort of the collective. However, the solutions lie in the effectiveness of security policies, policy enforcement, training, and cyber awareness.

Implications of Research Question RQ1b Findings. Compared to the problem presented in the other research question, the challenges of human-related issues in U.S. SMBs that make them fertile targets for cybercriminals can be solved in a specific period of time. To do so, business management must implement strong measures targeting employee mishaps and human errors. Participants believe that solid training programs with robust support systems will transform the current unsafe human–computer interaction of employees. In fact, the outcomes of cybersecurity training should be the practice of safe “habit” and “security culture.” Additionally, strict and applicable security policies must be firmly in place and enforced with disciplinary action. While these implications require businesses time and effort to plan and execute, the goals of eliminating employees’ mishaps and errors are realistically achievable with a strong leadership and organizational planning. The findings imply that by doing so, U.S. SMBs will appear to be less attractive in the eyes of intending hackers.

Analysis of Research Question RQ1c Findings. The current obsolete technological infrastructure in U.S. small and medium business was exclusively the concern of participants. This current state of technology infrastructure is regarded as the most significant technical barrier to all small and medium businesses. Believed to be the deadly vulnerability, this barrier generates numerous collateral technical issues and hardship in the workplace for employees. Unfortunately, business organizations seem to apply a believed-to-be quick fix to their outdated technological infrastructure, which creates a false sense of cybersecurity. For instance, organizations continuously patch up their almost decade-old software. This decision creates "recovery and redundancy issues," as mentioned by Participant 7. Furthermore, the findings suggest how the technological infrastructure is expected to be, according to real-world experiences of employees working in business organizations.

First, after upgrading, the new technological infrastructure must have the capability to stop popular cyberattack methods. Here, the keyword is *popular*, according to participants, U.S. SMBs are currently vulnerable to well-known and low-tech types of attacks. By fighting against commonly deployed types of attacks, the field of business would reject a vast number of cyberattacks such as DDoS and brute force. Interestingly, responses from participants indicate that they do not put high hope in a technological infrastructure that can fight off advanced and sophisticated attacks such as Stuxnet or NotPetYa through Medoc software, because the expenses for that high level of infrastructure are unbearable for SMBs. Second, in the context of obsolete technological infrastructure, the findings assume that human factor will always cause issues to cyber defense; therefore, the ideal infrastructure is expected to prevent cyberattacks resulted from employees' mishaps. This point is connected to responses addressing RQ1b. However, the findings approach employees' mishaps from a technical standpoint, rather than the

organizational resolution. Alarmingly, most participants have a firsthand account of cyber breach caused by their coworkers. As found, the suggested technical remedy for human error causing attacks is to have the infrastructure serving as a safety net for its stakeholders. More importantly, the findings imply that in case that technical safety net fail, it is expected, at least, to isolate the attacks and reduce damages. Above all, the bottleneck of solving the obsolete technological infrastructure are financial constraints. Assumingly, SMBs have limited financial sources due to their scale. Unfortunately, this limitation severely affects business leadership in the psychological sphere, as they view expenses for security as a burden rather than as an investment for their stability. While the limited financial resources are impactful, the wrong perspective of business decision makers about security investment prevents their organizations from overcoming challenges from limited budget to upgrade their infrastructure. Specifically, even with a small budget, SMBs are still able to patch their technical weaknesses with gradual and continuous investment, according to participants.

Implications of Research Question RQ1c Findings. Despite the financial constraints that are common with any SMBs, there are alternatives that organizations can take to circumvent these constraints. That is, as suggested by participants, to make small but effective cybersecurity investments to patch the biggest flaw in the cyber-defense system. The findings imply that the focus should be on technology shielding businesses from popular attack types and serving as the safety net in the event of cyberattacks caused by employees' mishaps. In other words, the findings suggest that SMBs should dedicate gradual investments into technical mechanisms preventing common cyberattacks and fending off cyberattacks caused by employees' mishaps and errors. More importantly, in order to have the previous suggestion realistically applied in SMBs, business leaders must change their mindset, labeled by three participants as "lack of

cyber knowledge," to view investments into cybersecurity as asset, rather than a burden. Surprisingly, the grassroot for the solution to technical barriers for a better cyber-defense capability lies in the point of view and mindset of business leaders of SMBs.

Analysis of Research Question RQ1d Findings. The findings of RQ1 are underlyingly connected to major problems in U.S. SMBs that have been revealed in other research questions. As indicated, participants frequently address the factor of funding and financial source in their answers. As a result, the answer to RQ1d concerning what practical cybersecurity mechanisms should be, surprisingly turns out to be outsourcing cybersecurity and mechanisms securing bring-your-own devices (BYODs). From the perspective of cybersecurity, outsourcing cybersecurity to third-party vendors is an appealing option for small and medium organizations. The findings shows that the main reason is third-party vendors have the dedicated security team with advanced cyber technology. Their sole job is to fight cybercriminals on behalf of contracting companies. Rather than SMBs with limited budgets and almost nonexistent knowledge of the cyberspace attempting to arm themselves with on-site security teams and expensive technology, third-party vendors are more efficient. Participants acknowledged that business organizations do not constantly scan threats, while third-party vendors always do. The findings suggest having a third-party vendor only under the condition that the vendor is suitable for the business organization. Furthermore, even with outsourcing cybersecurity to a third-party vendor, BYODs still pose threats to business organizations. Because of the special characteristics of these devices, which are personal computational machines connected to a business's network and managed by different level of employees' cyber awareness, the business organization is obligated to protect themselves from BYODs rather than relying on an outside vendor who protects the network from a comprehensive position. There are technical mechanisms

specifically addressed to reduce the threat and limit the impact once BYODs are hacked. These mechanisms are remote data eradication, technical validation, physical segmentation, network partition, and defined virtual access. The intentions of these mechanisms are not only to isolate BYODs but also to prevent data leaks. More importantly, in conjunction with technical mechanisms, certain non-technical measures were also considered, as technical mechanisms will not work when users are not following guidelines and policies. The findings recommend disciplinary action for violating organizational cyber policies while using BYODs.

Implications of Research Question RQ1d Findings. These findings offer a significant alternative to the current dire state of cybersecurity in U.S. SMBs. While the discussions in previous literature focus exclusively on reforming business organizations' cyber capability internally, these findings offer a fresh approach to reduce attacks with affordability. Indeed, with recommendations from real-world experiences of participants, SMBs can rely on third-party vendors to fight against cybercriminals efficiently and effectively. Nevertheless, this out-of-the-box approach to technical mechanisms has its limitations and risks. As stated in the discovered theme, business leaders must have eyes in choosing the appropriate third-party vendors to protect their precious but vulnerable asset. Relating to other findings in previous themes, choosing the appropriate vendor poses an enormous challenge due to the fact that there is a severe lack of cyber knowledge in SMBs. Mentioned by participants, an appropriate security vendor not only fits in the tight budget of an SMB but is also competent to battle against cyber perpetrators. Furthermore, preventing risks from BYODs is achievable for businesses. From a technical standpoint, most network infrastructures, including obsolete ones or decade-old operating systems, offer some form of segmentation. Participants strongly believed that, at the minimum, all business organizations must have network segmentation on different levels of the business

organizations. Relating to a problem revealed in RQ1b, creating practical security policies and strictly enforcing them to limit threats from BYODs can be an obstacle. Given the state of business leadership in SMBs, it requires time, effort, and commitment to implement BYOD security policies that encourage employees to voluntarily comply. Addressing this problem, the findings suggest that business decision makers start with addressing scope and procedure, then creating a framework covering the technical and organizational structure of the business organization. After all, the findings indicate that the endeavor for strong cyber-defense capabilities requires both appropriate technical mechanisms and effective organizational decision making.

Analysis of Research Question RQ1e Findings. Addressing RQ1e, it was clear that participants' concern about both internal and external impacts the cyber-defense capability of their organizations. Similar to other findings, when discussing about organizational mechanisms, minimal spending with highest possible return is the underlying drive. Witnessing U.S. corporations falling prey to cybercriminals through partnered companies, the findings indicated that small and medium businesses must defend themselves proactively and reactively. This includes being cautious with partnered businesses. The rationale from participants' responses is that when an SMB screens its partners for cyber flaws, that organization has already been successful in preventing a cyberattack before it happens. In application, the procedure is for the business to have or hire an independent cyber professional to conduct technology evaluation on the partnered company. For some SMBs, the more affordable option is to conduct interviews to assess their partners' defense posture. Of course, this alternative offers the less comprehensive illustration of partnered companies; however, the collected information provides fundamental facts for SMBs to prepare themselves. Equally important, cultivating and maintaining an

organizational culture for cybersecurity are the notable organizational mechanisms for securing a business from the inside out. Distinctive from the reviewed literature, participants focused particularly on the strategic relationship between IS professionals and other employees. The findings imply that, with that strategic relationship, security education is a continuous process that non-technical employees could learn from the IS professionals on a daily basis. This is an informal approach that could help small and medium business reduce large expenses in retraining for cybersecurity. This finding also indicates that there is an additional responsibility for IS professionals. Not only do they have to combat against threats and risk, but they must also become mentors, leading the human resources of a business organization to a better cyber-defense capability.

Implications of Research Question RQ1e Findings. Acquiring information on the cyber defense of partnered businesses can be a challenging task. It is the nature of business that internal and confidential information, particularly information systems, are not to be revealed to other companies, even business partners. However, this approach is gaining acceptance among U.S. corporations and businesses having contracts with the government, as any party in a contract must strictly adhere to the U.S. government's cyber regulations (Srinivas et al., 2019). Because attacks from third parties are unpredictable and difficult to defend (Kachgal, 2015), SMBs have to work around business barriers, such as refusal from partners, to gain as much information as possible to appropriately arm themselves with suitable measures. Regarding protecting an organization from the internal environment, a strong organizational culture for cybersecurity reduces the possibility of human errors causing cyberattacks. The effort to cultivate a cybersecurity culture falls on the shoulders of IS professionals, as they are the essence in the pandemic of ever-increasing cyberattacks against U.S. SMBs. A strong bond between IS

professionals and non-technical employees creates a strategic advantage for any business organization. With this additional role, the fundamental functions of IS professionals are mentor, supporter, and defender. Linking to other findings, business leaders are recommended to provide substantial support to IS professionals as, according to participants' feedbacks, IS professionals in SMBs are currently neglected. In essence, from the non-technical standpoint, cyber defense in SMBs is strong only when relationships among all stakeholders in business organizations are strong.

Relationship to Previous Studies and Anticipated Themes

Findings from this study correspond with the previous literature and the anticipated themes. Importantly, of the 13 themes derived from the collected data, two new findings emerged that were not addressed by the anticipated themes. These two themes are the age factor and outsourcing cybersecurity to third-party vendors. There were four subthemes obtained from the data analysis process. These four themes were addressed in the previous literature and the anticipated themes.

Research Question RQ1 Themes. There were three themes discovered from RQ1, which was "Why do small- and medium-sized businesses increasingly fall victim to cyberattacks?" These three themes are presented here. Theme 1 addresses technology deficiencies. Theme 2 pertains to the advancement of technology. Finally, Theme 3 addresses lack of knowledge. In reviewing the relationship of each theme to previous studies and anticipated themes, Theme 1 and Theme 2 are found to be addressed in the literature review, while Theme 3 is partially not consistent with previous research literature.

Theme 1: Technology Deficiencies. Consistent with the defense-in-depth approach (Byres, 2014; Presher, 2015) is the finding that a business organization with outdated technology

infrastructure, ranging from software and hardware to physical controls, results in a depleted cyber-defense capability leading to the increasing number of small- and medium-sized businesses falling victim to cyberattacks. In short, the defense-in-depth approach requires different domains of advanced technology to defend against cyberattacks in layers (Byres, 2014; Lai & Wu, 2015; Presher, 2015; Wolff, 2016). Therefore, having technology deficiencies deprives the defense-in-depth ability of U.S. SMBs. Similarly, refusing to update outdated technology is related to an issue found in the literature, specifically negligence in safeguarding critical infrastructure. While negligence in safeguarding critical infrastructure addresses the non-technical elements of cyber defense, this point is related to cyberattacks resulting from technology deficiencies by claiming that web-based attacks and information breaches connected outdated technology through disregarding cyber environmental factors and security activities (Safa et al., 2015). In other words, when U.S. SMBs do not pay attention to the current cyber environment that they are in, to update their technology accordingly, these business organizations are prone to be attacked.

Theme 2: The Advancement of Technology. Theme 2 concerns the advancement of technology and highlights that U.S. small and medium businesses are falling behind in the race of updating their technology leading to cyber vulnerability. This point was exclusively mentioned by Hayes and Cappa (2018), Petruzzelli and Sharma (2019), Smith (2018), and Jajodia et al. (2016). Specifically, the reviewed literature pointed out that the advancement of technology affects cyber defense in many elements. The reviewed elements are identifying risks, detecting vulnerabilities, disaster recovery and business continuity, and skill shortage. Importantly, both collected data and the literature review confirm that the development of new

technology resulting in more tech-advanced hackers puts U.S. SMBs in an uphill battle against cyber perpetrators.

Theme 3: Lack of Knowledge. Much of the previous literature has addressed the lack of knowledge in cyber defense from many perspectives. Bandler (2018) believed that cyber knowledge is utilized for updating and preparing for cyber threats. Taitto et al. (2018) supported the improvement of cyber knowledge for cyber resilience and responsiveness of businesses. Importantly, Principles 1 and 4 of the Control Objectives for Information and Related Technology (COBIT) 5 discussed slightly about the lack of knowledge regarding meeting stakeholders' needs through deploying new technology and using the combination of human-centered elements and advanced technology to select cyber-defense mechanisms for implementing the new business process. Importantly, the previous literature did not take into account "age" as a factor.

In the data collected from interviews, the participants perceived lack of knowledge differently from the reviewed literature. Specifically, the reviewed research did not consider the factor of age. However, participants believed that U.S. SMBs are often family owned, with old-school owners for whom the average age is higher. Relevant significant statements from participants were gleaned. These significant statements indicate that the lack of cyber knowledge because of age leads to the reliance on ineffective and old-fashioned business processes, no desire to prepare for cyberattacks, and the absence of cyber awareness. The consequences, according to participants, are that U.S. SMBs are prone to social engineering types of attack and technical intrusion.

Research Question RQ1a Themes. Research question RQ1a was "What are the existing types of barriers that impede enterprises from improving cybersecurity capabilities?" There were

two themes discovered for research question RQ1a. Theme 4 addressed the problems of human resources. Theme 5 regarded the lack of investment in cybersecurity. In evaluating the relationships of Themes 4 and 5, both themes are found to have been directly addressed by previous research literature.

Theme 4: Problems of Human Resources. Participants demonstrated the challenge of lacking cyber human resources through complaints of being understaffed in the IT department, facing overwhelming technical issues to be solved, and lacking accessibility to hiring cyber professionals and other related matters. Specifically, the collected data perceives the current problem of human resources is consistent with Petruzzelli and Sharma (2019) and Smith (2018). Their research concluded that the lack of human resources in the cybersecurity field leads to the eminent cyber threat for U.S. SMBs. Similarly, the point that participants expressed regarding the frustration of overwhelming technical work at their business organization is equivalent to a finding of Smith that 70% of cyber professionals are severely impacted by the lack of cybersecurity workers in their workplaces. Additionally, the claim that emerged from the collected data regarding the problem of cyber human resources in U.S. SMBs is identical to the dilemma identified in previous research.

Theme 5: The Lack of Investment in Cybersecurity. The findings from the data collected affirm the deficiency of investment for cybersecurity in U.S. SMBs. Two elements specified in the data are technology upgrade and human resources, both affected by the lack of investment. These elements were also thoroughly investigated and alarmed by Hawkins (2017) and Gordon et al. (2015). Many participants believed that if the lack of investment tendency in U.S. small and medium businesses continues, these business organizations are anticipated to become the future target of cyberattacks. This point is consistent with the findings of Fielder et al. (2018), who

claimed that the less investment SMBs direct toward cybersecurity, the more vulnerable they are to cyberattacks.

Research Question RQ1b Themes. Research question RQ1b was "How impactful are organizational barriers on small and medium enterprises in improving their cybersecurity capability?" For this research question, three themes were discovered. They are "the human factor is the weakest link," "the less training and support, the more depleted cybersecurity capability," and "security policies." These three themes were found consistent with the reviewed literature. Specifically, they are corresponding with reviewed literature addressing cyber defense.

Theme 6: The Human Factor Is the Weakest Link. Collected data indicates that the human factor will always be a problem for defending the cyber system in U.S. SMBs. This point is identical to the finding of Kemper (2019), who found that 90% of cyberattacks are originated from human factor. More succinctly, participants did not have the confidence that the dilemma of human error resulting in cyber breaches will be solved in the near future. Supporting this point, Newmeyer (2015) concluded from his study that there is a lack of analysis ability in U.S. businesses' human resources, which leads to human factor as the weakest link in cyber defense. As a result, there is an enormous gap for U.S. businesses to solve between human analysis ability and cyber-threat landscape.

Theme 7: The Less Training and Support, the More Depleted Cybersecurity Capability. Participants showed a strong support for cybersecurity training in U.S. SMBs. This point aligns with much of the reviewed literature, as training optimizes cyber expenses (Krishan, 2018), reduces phishing attacks (Alsharnouby et al., 2015), improves awareness (Korpela, 2015), and limits human error (Marquardt, 2019). It is significant to note that the majority of respondents evaluated current training programs in their business organizations as ineffective. Supporting this

response, Caldwell (2016) concluded that only 33% of surveyed employees rated their cyber training as effective. Additionally, participants' emphasizing the importance of having a support system to maintain the effectiveness of cyber training is similar to recommendations of Hanus and Wu (2016). Both reviewed literature and collected data strongly support the statement that the less training and support, the more depleted cybersecurity capability.

Theme 8: Security Policies. Both collected data and reviewed literature support the implementation of tough cybersecurity policies in business organizations (Kemper, 2019). Importantly, participants reported the absence of implemented security policies or having inapplicable policies in small and medium business. This point was not addressed in previous research. Distinguishably, participants viewed security as the baseline for business growth and an organizational challenge in terms of cyber defense. By contrast, the reviewed literature focuses on security policies from the standpoint of operational defense and governmental regulations.

An emerging subtheme is that both the collected data and the reviewed literature agreed that training and security policies have to be implemented simultaneously to accomplish cybersecurity goals through cyber awareness in business organizations. While participants and previous research support the improvement of cyber awareness through training and security policies, the approaches between these two sources of information are distinctive. In raising awareness, participants indicated the application of training and policies based on management level and specific job role with being constantly reminded of security standards through different channel of communication. In the reviewed literature, intentions for training and security policies were to start from the top-down approach (Kemper, 2019). Training and security policies influence behavioral change and sensitivity of employees (Trim & Lee, 2019) and comply with governmental regulations (Srinivas et al., 2019).

Research Question RQ1c Themes. Research question RQ1c was "How impactful are technical barriers on small and medium enterprises in improving their cybersecurity capability?" For this research question, there was only one theme discovered, which is obsolete technological infrastructure. Importantly, participants discussed this theme in depth through different lenses. There were three subthemes discovered from the main theme of obsolete technological infrastructure. These three subthemes are financial constraints, the incapability of existing technology in preventing common cyberattacks, and the inability of existing technology to prevent cyberattacks originated from human error.

Theme 9: Obsolete Technological Infrastructure. Respondents discussed in-depth the outdated technology at their business organizations. Specifically, old hardware and software were of the most concern, as they have severe impact on the daily work of participants. This perspective is consistent with the findings of Jajodia et al. (2016). Regarding software, both the reviewed literature and participants believed that patching and updating are the short-term solution for applications in obsolete technical infrastructure (Ge et al., 2018). Furthermore, any hardware that reaches age limits is required to be replaced, according to participants. This sentiment is shared by Wagner (2016) and Cho and Ben-Asher (2018), because hardware is interconnected to software and has a prominent impact on the cyber capability of an SMB.

Subtheme: Financial Constraints. Constraints of financial resources are the main drive that makes U.S. SMBs keep their obsolete technological infrastructure, according to participants. This point is found consistent with Hawkins (2017), who concluded that budget constraints are making SMBs vulnerable in the cyberspace. Similarly, participants identified the use of obsolete systems. Budget is regarded as the biggest challenge for cyber capability. Sharing this point,

Fielder et al. (2018) believed that the less money invested in cyber defense, the more financial damages occur to U.S. SMBs.

Subtheme: Existing Technology Is Incapable of Preventing Popular Cyberattack Methods. Collected data showed that the existing outdated systems cannot prevent popular cyberattacks. There were five attack methods mentioned by participants: malicious software, DDoS, password attack, phishing and spear phishing, and eavesdropping. Besides eavesdropping, the other four attack methods were specifically addressed in the reviewed literature. The previous reviewed research did address data breach, the category under which eavesdropping attack falls. Furthermore, participants discussed dividing employees into different sensitivity levels to prevent common attack methods. This point was somewhat addressed in the literature addressing risk management. Specifically, the cybersecurity triad—confidentiality, integrity, and availability (Ioannidis et al., 2019)—and implementing strategic changes in technology-related human resources (Sanders & Spiering, 2016) support participants' perceptions of dividing employees into different levels of network sensitivity.

Subtheme: Existing Technology Should Be Able to Prevent Cyberattacks Originated From Employees' Mishap. Participants believe that when human error causes a cyberattack, the implemented technology should be able to serve as a safety net. This belief is supported by Moghimi and Varjani (2016) and Azhagiri et al. (2017). Sharing the same perception of the inability of technology preventing attacks from human error with collected data, Azhagiri et al. revealed that U.S. SMBs are experiencing limited implementation of multilevel cyber-defense technology. Furthermore, the capability to isolate threat was discussed in the collected data. This point is consistent with Byres (2014), who recommended that business organizations install appropriate technology to isolate incoming attacks.

Research Question RQ1d Themes. Research question RQ1d was "What are the practical cybersecurity mechanisms that could boost the cyber-defense capabilities of small- and medium-sized businesses?" There were two themes discovered for this research question. They are outsourcing cybersecurity and bring-your-own devices (BYODs). The theme of outsourcing cybersecurity is a new finding. The theme of BYODs is found to be consistent with the body of existing literature.

Theme 10: Outsourcing Cybersecurity. Outsourcing cybersecurity to third-party vendors is a newfound theme. The body of literature did not address participants' support for outsourcing cybersecurity matters in U.S. SMBs to third-party services. In the collected data, participants pointed out that choosing the appropriate third-party security vendors would save cost for two reasons. These are eliminating the on-site cyber team and better cyber assurance. Approaching the matter of cutting cybersecurity cost, the reviewed literature, on the other hand, recommends that low-budget companies train for cyber awareness with realistic scenarios (Korpela, 2015; Miranda, 2018). Additionally, Ransbotham et al. (2017) pointed out that many U.S. SMBs are adopting artificial intelligence (AI) technology as a means to cut cybersecurity cost. Other than the two suggestions from the body of the literature regarding cutting cybersecurity costs in businesses, there was no indication that recommends the trend of using third-party cybersecurity services, as thoroughly discussed by participants. Comparing previous research on this issue with the collected data from the present research, besides two recommendations—specific training program and AI technology— the reviewed literature focused more on the financial cost in the aftermath of cyberattacks.

Theme 11: Bring-Your-Own Devices: Policy and Network Segmentation. The concern with bring-your-own devices (BYODs) was discussed exhaustively by participants, as data leak

is the main possibility. This sentiment is shared by Baillette and Barlette (2018) and Qamar et al. (2019). Besides data leaks, the reviewed literature also addresses concerns about malware attacks against BYODs (Furnell & Dowling, 2019; Malatji et al., 2019; Visu et al., 2019). Furthermore, the collected data indicates a major support for network segmentation as a means to reduce risks from BYODs. This point is consistent with Friedberg et al. (2015) and Azhagiri et al. (2017), who support network partitioning in combination with detection analysis.

Research Question RQ1e Themes. Research question RQ1e was "What are the practical organizational mechanisms that could boost the cyber-defense capabilities of small- and medium-sized businesses?" For this research question, Themes 12 and 13 were discovered. They are evaluation on risks from third party and cultivating an organizational culture for cybersecurity. These two themes focus on the non-technical approach for improvements of cyber vulnerabilities in business organizations. Both themes were found corresponding with the body of the literature and anticipated themes.

Theme 12: Conducting Evaluation on Risks From Third Party. The collected data recommend that U.S. SMBs conduct thorough evaluation of risks from third party. This recommendation is also supported by Kure et al. (2018), who suggested that business organizations evaluate risks that stakeholders may have on the organization's physical and digital infrastructure. Furthermore, the response recommending evaluating risks from third party is aligned with the cyber-disaster recovery plan of Kachgal (2015), as he suggested that business organizations should scan the external environment of the organization for a better recovery after any cyberattacks. From a general point of view, this theme also fit into Tounsi and Rais's (2018) conclusion that the ability of a U.S. SMB to recover quickly in the aftermath of a cyberattack depends greatly on threat intelligence acquired from the risk assessment process.

Theme 13: Cultivating an Organizational Culture for Cybersecurity. Participants discussed exclusively about open communication and formulating and maintaining strategic relationships between employees, especially between IS professionals and other employees. These two factors were mentioned as the essence for cultivating an organizational culture for cybersecurity. The point of open communication is found consistent with a component listed for making organizational changes for improved cybersecurity ("Succeeding With Organizational Change," 2015). Also, Humayed et al. (2017) mentioned communication as one of the three significant components required for a strong physical defense in the cyberspace. Additionally, Kachgal (2015) believed that communication is the key for organizational cyber resiliency in terms of recovering after cyber disaster. Furthermore, the element of maintaining strategic relationships between employees, especially between IS professionals and other employees, is aligned with recommendations and perspectives of multiple previous research. Hayes and Cappa (2018) shared the same sentiment, that IS professionals have the direct impact on the security posture of an organization. Similarly, addressing the point of maintaining strategic relationship between employees, Ukil and Akkas (2017) revealed that the benefits of doing so are implementing strategic cultural changes effectively, including technology adoption to mitigate current and future cyber risks.

Summary of the Findings

Thirteen themes were discovered based on the six research questions through the data collection process in this research study. These themes offer a realistic perspective into the current dire situation of cyber-defense capability in U.S. SMBs. For research question RQ1, there were three themes discovered. They are technology deficiencies, the advancement of technology and the lack of knowledge. These themes revealed the answers of why U.S. SMBs

increasingly fall victim to cyberattacks. Furthermore, the two themes: problems of human resources and the lack of investment in cybersecurity were the major discovery for research question RQ1a. These two themes exposed the existing types of barriers that impeded U.S. enterprises from improving cybersecurity capabilities. These revealed existing types of barriers indicated that human factors are the main elements impeding U.S. SMBs from improving cyber defense capabilities. Focusing on organizational factors of cyber defense, research question RQ1b sought to discover how impactful organizational barriers are on U.S. SMBs in enhancing cyber defense. There were three themes derived from the collected data that exposed the significant impact of organizational barriers. Discovered themes were the human factor is the weakest link, the less training and support, the more depleted cybersecurity capability, and security policies. Together, these themes covered the non-technical dimension of cyber defense in business organizations. Correspondingly, research question RQ1c addressed the impact of current technical barriers in businesses. There was one theme discovered, which was obsolete technological infrastructure. Notably, this theme included three subthemes that detailed the dilemma U.S. SMBs are facing. These subthemes were financial constraints, existing technology is incapable of preventing popular cyberattack methods, and existing technology should be able to prevent cyberattacks originated from employees' mishap. These subthemes evidenced that U.S. SMBs are extremely vulnerable to cybercriminals. Besides uncovering both technical and organizational barriers for the better cyber defense, there were themes derived from the data collection proposing the realistic remedies for the depleted cyber defense in U.S. SMBs. Research question RQ1d explored the practical cybersecurity mechanisms that could boost the cyber-defense capabilities of small- and medium-sized businesses. Outsourcing cybersecurity and bring-your-own devices: policy and network segmentation were the two themes discovered

from the data analysis process. These two themes addressed the practical cybersecurity mechanisms that U.S. SMBs could rely on boosting the cyber-defense capabilities. Finally, research question RQ1e focused on practical organizational mechanisms. Specifically, the two themes, conducting evaluation on risks from third party and cultivating an organizational culture for cybersecurity, discussed how business organizations could patch the human errors existing in their organizations. In conclusion, the findings addressed meticulously both contemporary technical and organizational barriers in business organizations for a strong defense capability. By doing so, the findings have answered at length various categories that research questions seek to discover. These categories are the reasons behind SMBs continually falling prey to cyberattacks, the impacts of organizational and technical barriers, and the technical and organizational mechanisms that organizations are expected to equip and implement for a robust defense system. In short, the discovered findings not only expose the realistic problem currently existing in U.S. SMBs through the eyes of participants working there, but also propose the ideal mitigations for hardships that businesses are facing.

More succinctly, the findings have successfully addressed the research problem of this study by covering a wide range of substantial elements and current issues. By exposing those elements and issues, the findings have connected the gap of previous research addressing both the business field and the cybersecurity field, as there is a lack of reports and findings about cyberattacks and vulnerabilities in the private sector (Denning & Denning, 2016), let alone specifically U.S. SMBs. The discovered themes serve as the detailed answers to the problem that has been ignored for a long time: the growing number of cyberattacks critically threatening SMBs of the U.S. private sector. Particularly, the findings address the research problem from multiple angles based on the experiences of participants, revealing elements related to the

problem from both business and technical levels. These angles are technical dimension, organizational dimension, management framework, internal environment, and external environment. In short, the findings cover well beyond what might be expected from an investigation of the problem of U.S. SMBs continuing to fall prey to cybercriminals.

Given that the purpose of this study was to reveal the contemporary barriers and challenges that impact the latest cybersecurity competencies of U.S. small and medium enterprises, the findings illustrate precisely the hardship that these businesses are facing in the losing battle against cybercriminals. As revealed, there are existing technical factors and organizational elements posing as barriers and challenges for a better cyber capability. Unsurprisingly, participants have firsthand accounts of numerous attacks. Distinctively, because the majority of existing studies focuses on the issues of cyberattacks in the business field with either technology-assisted attacks or technology-focused attacks (Donalds & Osei-Bryson, 2019), the findings offer a whole new perception to the problems of cyber defense in SMBs by exposing risks and threats through both technical and organizational lenses. As a result, the findings have successfully served the purpose of providing the breakthrough information that could initiate changes in business organizations to defend against the ever-increasing number of cyberattacks in the business sector.

Application to Professional Practice

The purpose of this qualitative research study was to explore the current challenges and barriers impacting cyber-defense capabilities of U.S. small and medium-sized businesses. Several themes were discovered through collecting data from employees who are currently working for small and medium-sized businesses. In addition, participants also revealed numerous business practices that they deemed vulnerable for companies. The end goal of this study was to

provide SMBs with breakthrough information that could initiate improvements of the cyber defense. Based on discovered themes, the section below discusses two significant approaches. First, the section on improving general business practice provides a thorough discussion of how the results of this qualitative research can improve current business practices. Second, the discussion on potential application strategies provides details on how U.S. small and medium-sized businesses can leverage the findings of this study to reduce cyber threats and mitigate cyberattacks.

Improving General Business Practice

The result of this qualitative study provides a significant improvement to general business practice, particularly from the themes discovered during collecting data from employees currently working for U.S. small and medium-sized businesses. All themes indicate contemporary cyber weaknesses of the majority of SMBs. Through the study results, it is clear that with regard to cybersecurity, the current general business practice is highly harmful to the cyber defense of SMBs. To improve the general business practice, there are two approaches that SMBs should urgently follow to minimize the possibility of becoming the next cyber victim. Regarding business cybersecurity, these approaches are general business practice for better organizational defense and general business practice for better technical defense.

General Business Practice for Better Organizational Defense. With regard to the cybersecurity perspective of the current general business practice, there are many improvements companies should urgently carry out. According to Kemper (2019), human factors lead to 90% of cyber breaches. This statistical number corresponds with data provided by participants. Alarmingly, all participants admitted that their companies are highly vulnerable in terms of organizational defense. Answers shared by participants and their anecdotes signified that

cybercriminals are more likely to take advantage of organizational flaws in the current business practice to attack and exploit the digital assets and valuable data. Particularly, the findings of this study pointed out seven overwhelming organizational weaknesses of business practice in SMBs. They are the lack of cyber knowledge, problems of human resources, human errors, training and support, security policies, conducting evaluation on risks from third party, and cultivating an organizational culture for cybersecurity. These seven themes offer not only relevant insights to existing cyber risks in businesses across industries but also applicable recommendations to stakeholders in companies. Importantly, IS professionals and organizational leaders are the two foremost subjects who benefit the most from the results of this study. IS professionals and organizational leaders are the decision makers who have the strong impact on cyber-defense capabilities of companies. The result of this study pointed precisely to areas that IS professionals and business leaders can focus on to improve the general business practice for better organizational defense. Furthermore, the result of this study also reminds businesses, regardless of size and industries, that cyber vulnerabilities are possibly lurking in their organization and they could already be in the aim of cybercriminals. Therefore, the vital solution is to improve business practice based on the revealed study results to minimize the possibility of becoming a cyber victim or to effectively mitigate impacts of cyber exploitations.

General Business Practice for Better Technical Defense. As important as organizational defense, technical defense is also the frontline of any company in the fight against cyberattacks. While technical capability and information system vary between businesses and industries, the findings of this study pointed out the major technical flaws existing in U.S. small and medium-sized businesses. There are six themes revealing the existing technical flaws in the current business practice. They are technology deficiencies, the advancement of technology, the

lack of investment in cybersecurity, obsolete technological infrastructure, outsourcing cybersecurity, bring-your-own devices: policy and network segmentation. Cyberattacks are becoming increasingly more sophisticated and cyber loss continues to rise, according to participants. Business owners and organizational decision makers must be alerted to take initiatives to tackle possible cyberattacks. The results of this study serve the purpose of alerting business owners and decision makers that their technical capability is obsolete and unmatched for the common attack methods. This study improves the general business practice by bringing cyber awareness to small and medium businesses for which participants claimed that owners and decision makers have no knowledge of cybersecurity or disregard their current cyber defense.

Potential Application Strategies

U.S. small and medium-sized businesses can use the potential strategies derived from the discovered themes to improve both organizational and technical defenses. The potential strategies are highly recommended to apply in companies as these strategies are acquired from analyzing the collected data meticulously. Importantly, the collected data is the concerns, perspectives, and insights of various IS professionals working in small and medium businesses across industries in the United States. The potential application strategies approach the issues of cybersecurity in organizations with two dimensions: organizational and technical. These approaches provide a strong solution for a better defense capability because cybersecurity requires both human factors and technical elements. There are three strategies that U.S. companies are recommended to use to leverage the findings of this study. They are cultivating a cybersecurity culture, selective investment in technology, and frequent evaluation of cyber risks.

Cultivating a Cybersecurity Culture. Cybersecurity requires the efforts of two elements: people and technology. Feedback from all participants indicates that having a

cybersecurity culture is the winning element in the battle against cyberattacks. Based on collected data, a cybersecurity culture requires the involvement of not only business leadership but also all levels of employees. Some participants included external elements such as business partners and vendors in defining a cybersecurity culture. Because of the alarming human errors, lack of knowledge, and technology deficiency, cultivating a cybersecurity culture is considered as the most applicable strategy in defending companies' cyber infrastructure. Cultivating a cybersecurity culture is the most applicable strategy, based on data collection. The reason is that this strategy requires less spending than upgrading the entire technology systems while having a long-term impact. The main long-term impact is that employees have a habit of protecting digital assets and a high level of cyber awareness. Training and support are particularly considered the foundation for cybersecurity culture.

Training and Support. The purpose of training programs and continuous support is to equip employees with cyber knowledge, form safe habits, raise awareness, and maintain safe business practices. Companies are recommended to schedule training programs once a year or quarterly. Importantly, an effective training program must involve all stakeholders including business leaders, combine training elements to business mission, and continue developing training elements based on business strategy and technology circumstances. Equally important, a company must have a continuous support to remind stakeholders of cyber hygiene and to form a habit of cyber safety. Open communication and formulating and maintaining strategic relationships between employees are considered the backbone of continuous support.

Selective Investment in Technology. All participants claimed that their organizations have outdated technologies. This problem is the significant concern for defending enterprise systems against cyber intrusion and exploitation. For small and medium-sized businesses, any

decision made can greatly impact their organization, especially budget. Therefore, as mentioned by the majority of participants, the foremost strategy businesses must focus on is to upgrade their technical infrastructure selectively. By selecting strategically which part of the technical system to upgrade, companies have the benefits of avoiding major spending while partially securing the infrastructure from risks. Data analysis indicates that this strategy will effectively lower the risks of common attacks such as ransomware and data thief, decrease IS employees' workload, and improve business process. Interestingly, from a business perspective, this strategy increases the market competitiveness of companies.

Frequent Evaluation of Cyber Risks. The result of cyber risks evaluation provides companies with valuable information on how vulnerable they are and brings awareness to business leadership. None of the participants' organizations conduct evaluations of cyber risks. The rationale for cyber-risk evaluation is that spending time and effort on checking both the systems and business practices is cost-effective than dealing with a cyber loss and the costs to recover. This strategy is effective and applicable in proactively defending against possible cyberattacks because detection, understanding of the situation, and acknowledging the impact assessment on the future are the key elements for businesses to plan their defense parameter (Pöyhönen et al., 2019).

Summary of Application to Professional Practice

The results of this study indicate that U.S. small and medium-sized businesses are far behind in the never-ending battle against cyberattacks. There are recommendations for improving the general business practice. The improvements for better general business practice are broken down to two dimension: organizational and technical, because they are the two foundations of a business's cyberspace. Both organizational and technical sections discuss at

length how the results of this study can improve the general business practice by zooming in on cyber weaknesses that are currently endangering SMBs. Furthermore, the potential application strategies discuss in detail what strategies U.S. SMBs are highly recommended to implement urgently. They are cultivating cybersecurity culture, selective investment in technology, and frequent evaluation of cyber risks. Because of financial constraints, human factors, obsolete technology, and the overall situation of U.S. SMBs, these strategies are believed to be applicable and effective, according to participants.

Recommendations for Further Study

This section focuses specifically on two areas that should be studied based upon the findings of this study. The two areas are financial resources and cyber defense, and relying on the third-party cybersecurity. These two areas became recommendations for further study based on how participants responded to the interview questions. Participants put the blame on financial resources for the challenges they are facing and mentioned multiple times that third-party cybersecurity services are a possible solution for the dire situation of cyber defense in U.S. small and medium-sized businesses.

Financial Resources and Cyber Defense

Budget, expenses, and financial resources are the key words in data collection. It is expected as small and medium businesses often do not have a large budget, let alone a large budget for cybersecurity. However, financial resources and its relation to cyber defense is critical to be researched further, as participants often claimed that budget is a big issue for cyber defense. On the other hand, human errors are also claimed to be a vital element resulting in a cyberattack. These two points are somewhat contradictory. Therefore, it is suggested that financial resources and cyber defense is an area worth meticulous study. Particularly, a future study could

investigate whether budget has a direct impact on cyber defense or human errors contributes predominantly to cyberattacks. The ground for the suggested future study is that SMBs are attacked because of limited budget or because of their human errors.

Relying on the Third-Party Cybersecurity

A majority of participants brought up the idea of having a third-party cybersecurity service as a solution to have better experts addressing cyber defense in SMBs and to cut the cost of cyber defense. However, some participants were skeptical about this solution and suggested that SMBs should be due diligent in choosing a third-party cybersecurity service. It is important to weigh the option of having a third-party service oversee cyber defense based on two grounds. These two decisive elements are costs and expertise. SMBs may have to spend more for working with a third-party service or the other way around. In addition, the suitability of the third-party service is highly important. Depending on the industry, technology infrastructure, and other related factors, the option for the third-party service can be effective or a waste of money. A further study of this area is highly suggested based on many elements that the fields of cybersecurity and business have not addressed. To name a few, they are the variety of third-party cybersecurity service, the cost of having a third-party service and having an onsite security team, and the effectiveness in combating cyberattacks. The expectation for further study is to provide not only the answer as to whether SMBs should rely on a third-party cybersecurity service but also insight into various elements such as costs, how dependent SMBs should be on the third-party service, and the effectiveness of mitigating risks and attacks.

Reflections

This section is an opportunity for the researcher to discuss highly valuable information beyond the topic of cybersecurity and business. First, the researcher will reflect on how the

research process and the study research have provided the researcher with personal and professional growth. Second, the biblical perspective section discusses in detail how this study is related to a Christian worldview and the theology integrated in the study result. There are two sections addressing this biblical perspective: how business improves the lives of God's children and the fierce battle between good and evil.

Personal and Professional Growth

Throughout the journey to complete this study, there has been significant growth as a person, student, and business decision-maker for the researcher. So far, all dissertation tasks have been very challenging for the researcher. However, the most pessimistic time for the researcher was during the completion of tasks 12 and 13. There were numerous seemingly insurmountable challenges to the level that the researcher was about to give up. These challenges came from personal life, work, and limitations to complete those dissertation tasks. The researcher sent out multiple invitations to solicit participants for the study, approximately 50 candidates. However, there were only a few responses. The researcher believes that candidates are hesitant to participate due to the nature of the field of cybersecurity. They may be concerned that giving out information on cyber vulnerabilities could jeopardize their employment and business organization. Despite explaining in detail in the invitation letter and mentioned informally before each interview, all participants asked how their answers would be used and if their personal information would be disclosed. Fortunately, through snowball sampling, the researcher was able to collect enough data to reach saturation. Looking back at hardships, both in life and academic, the researcher learned a lesson that when facing an obstacle, the first step is to break it down into smaller pieces to solve that obstacle with different approaches while momentarily forgetting everything else besides that obstacle, in order to exclusively focus on the solution. The

researcher also believes that God was the One who not only gave him the challenge but also the strength to persist and the wisdom to overcome. Therefore, challenges, both in life and school, are blessings for personal growth. Furthermore, the researcher gained a substantive understanding of business cybersecurity. Conducting this research study illustrates a bigger picture of the relation between cybersecurity and business, more than from the perspective of an IT employee, which was the researcher's past experience. Starting from the time of writing the literature review in this research study, the researcher as a business decision maker in a company has implemented multiple measures focusing on preventing social engineering attacks and digital access control due to the alarming information found while reviewing past literature. Unfortunately, the researcher's organization suffered from a social engineering attack from which the loss was $4,000. Combining this incident and the result of the study, the researcher learned a valuable lesson that the entire business organization can be jeopardized through the lowest level employees who have no access to semi-confidential data.

Biblical Perspective

Our Heavenly Father created "the heaven and the earth" (Genesis 1:1). This world and everything that it contains belong to our Creator. Thus, no matter the subject, all things have a divine meaning since the beginning of the creation, including business and cybersecurity. To be clear, cybersecurity in this sense does not mean solely the internet but the biblical value beyond cyber and security. These values are the protection for the improvement of God's children through business, the fight between good and evil, God's commandments for mankind. As God's intention is the essence of life, the section below discusses those values from biblical perspectives that can be utilized as the ethical frameworks for the daily work of IT professionals and the moral pillars for business in improving their cyber defense.

Business Improves the Lives of God's Children. It is inarguable that business improves people's lives. Business contributes greatly to the improvement of society by providing goods and services and continuously inventing new ways of improving the quality of products and services. The evidence is that, when looking at countries in the world, the higher the quality of life and the wealthier a country, the more prosperous business there are in different sectors. With that being said, it was the divine intention to create the field of business as an avenue for the betterment of God's children (Keller & Alsdorf, 2014). This scripture addresses this intention as "The Lord God took the man and put him in the Garden of Eden to till it and keep it" (Genesis 2:15). It means that God gave His children (businesses) specific work to do, both physical work and intellectual work. Therefore, all the work we do is rooted in God's design for humanity. Thus, any disruptions to the divine purpose of having His children (businesses) to do the work must be eliminated. The field of cybersecurity and particularly this research study attempt to prevent business cyber disruptions, which is related and integrated with a Christian worldview. Specifically, this research study is an honor to serve God's intention by alarming businesses with the existing vulnerabilities and promoting safe business practices in the cyberspace. By doing so, businesses can better fulfill God's purpose for them on earth by being more secured against cyberattacks and ensuring that their growth is not plundered by criminals. In order words, the result of this study helps God's children (business) work as God's design without being disrupted by evil (cybercriminals).

The Fierce Battle Between Good and Evil. The battle between good and evil has been going on since the beginning of time (Genesis 2:1-25). In this era of technology, the cyberspace has become a battleground between good and evil. On this cyber battleground, businesses are struggling at every moment to fight off vicious cyberattacks. This is especially true of U.S. small

and medium businesses. In this fight, the field of cybersecurity is the divine armor for which it will stand against the schemes of the devil (cybercrime) (Ephesians 6:11 ESV). Interestingly, from the theological view and cybersecurity perspective, IT professionals and cybercriminals perfectly represent the scale of good and evil. The two groups have similar wisdom, knowledge, and expertise. Unfortunately, one chooses to protect while the other chooses to steal and "murder." Indeed, cybercriminals violate many commandments of our Heavenly Father. Foremost, they violate the commandment of not stealing (Leviticus 19:11) and not murdering (Matthew 19:18). In fact, the aftermath of most cyberattacks is often financial loss, up to $8.6 million per company (Stanciu & Tinca, 2017). In other words, the evil in the context of business cybersecurity steals the fruit that companies have grown with their sweat and tears. Cybercriminals not only steal but they also "murder." With every successful attack, they murder the hopes and dreams of business owners and many other stakeholders who depend on the prosperity of the attacked business. Having a closer look at attacks and business, the cruelty of cybercriminals intensifies when 72% of cyberattacks target U.S. small and medium businesses (Fielder et al., 2016). This means that the evil goes after the most vulnerable organizations in the business sector. These organizations are mom-and-pop businesses or a business startup belonging to someone putting everything into it to have it up and running. Thus, cyberattacks take away the hopes and dreams of many of God's children in the business sector.

Summary of Reflections

The section of reflections addresses how the research project provided the substantial growth for the researcher and biblical perspective of the study. In terms of personal growth, challenges and hardship have strengthened the researcher in various aspects to be more confident in tackling future difficulties. For professional growth, the researcher was equipped with latest

data of business cybersecurity. This inspires the researcher to initiate changes and implement measures to better safeguard his organization from cyberattacks. The discussion of the biblical perspective addresses various aspects of business and cybersecurity based on a Christian worldview. Particularly, God's intention for business was examined, noting that disruption of the work of business goes against His design. By analyzing cybersecurity in business through the theological scope, the effort of companies in defending their systems against cyberattacks is related to a foundational theology. That is the fight between good and evil.

Summary of Section 3

This qualitative research studied the ever-increasing number of cyberattacks in U.S. small and medium businesses. The section of presentation of the findings revealed the ongoing issues and challenges for U.S. SMBs in fighting against cyberattacks. There were seven participants who took part in the data collection process. A total of 13 themes was discovered, which covered both the organizational and technical aspects of cybersecurity and business. Further, the findings were compared and contrasted against three conceptual frameworks, research questions, and previous studies and anticipated themes. The purpose was to attain a detailed picture of the relationships between the findings and each of the three pillars.

Furthermore, the application to professional practice section discussed the applicability of the findings through two sub-sections: improving general business practice and potential application strategies. The study's results showed that there are critical cyber improvements that businesses are urgently recommended to implement. These improvements span both technical and organizational realms of cybersecurity for better business practice. In terms of application strategies, there were three recommended strategies that the collected data indicated would improve businesses' cyber defense. These strategies are cultivating a cybersecurity culture,

selective investment in technology, and frequent evaluation of cyber risks. Notably, the recommended strategies and recommendations for further studies are somewhat similar. They were both based on the nature and technology circumstances of U.S. small and medium businesses: small financial capability and using outdated technology. Last, in the reflection section, the researcher reflected on how the research project developed the researcher substantially in both personal and professional growth. The growth was achieved through overcoming challenges and implementing new business strategies based on information learned from this study. Importantly, the biblical perspective of this research study was thoroughly analyzed and discussed. The fundamental points of the biblical perspective in this study are to serve God's intention by protecting business and to define the relation between business cybersecurity and the fight between good and evil, as mentioned many times in the scripture.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Alammar, F. M., Intezari, A., Cardow, A., & Pauleen, D. J. (2019). Grounded theory in practice: Novice researchers' choice between Straussian and Glaserian. *Journal of Management Inquiry*, *28*(2), 228–245. https://doi.org/10.1177/1056492618770743

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

Alkhaldi, F. M., Hammami, S. M., & Uddin, M. A. (2017). Understanding value characteristics toward a robust IT governance application in private organizations using COBIT framework. *International Journal of Engineering Business Management*, *9*(1), 184797901770377. https://doi.org/10.1177/1847979017703779

Allen, J. (2017). Surviving ransomware. *American Journal of Family Law*, *31*(2), 65–68.

Al-Matarneh, F. M. (2020). Advanced persistent threats and its role in network security vulnerabilities. *International Journal of Advanced Research in Computer Science*, *11*(1), 11–20. https://doi.org/10.26483/ijarcs.v11i1.6502

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet and Information Systems*, *12*(2), 747–763. https://doi.org/10.3837/tiis.2018.02.012.

Alnusair, A., Zhong, C., Rawashdeh, M., Hossain, M. S., & Alamri, A. (2017). Context-aware multimodal recommendations of multimedia data in cyber situational awareness. *Multimedia Tools and Applications*, *76*(21), 22823–22843. https://doi.org/10.1007/s11042-017-4681-2

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Amali, L. N., Katili, M. R., Suhada, S., & Hadjaratie, L. (2020). The measurement of maturity level of information technology service based on COBIT 5 framework. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, *18*(1), 133–139. https://doi.org/10.12928/telkomnika.v18i1.10582

Amao, M. (2015). *Active cyber defense to fight cybercrime* (Publication No. 1606336) [Master's thesis, Utica College]. ProQuest Dissertations & Theses Global.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Anomah, S., & Aduamoah, M. (2018). Proposed analytical procedure for the customization and implementation of Cobit 5, an auditing tool: An action design research approach. *EDPACS: The EDP Audit, Control, and Security Newsletter*, *57*(3), 15–34. https://doi.org/10.1080/07366981.2018.1433933

Anstee, D. (2015). Preparing for tomorrow's threat landscape. *Network Security*, *2015*(8), 18–20. https://doi.org/10.1016/S1353-4858(15)30072-6

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. F. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *Qualitative Report*, *22*(6), 1607–1621. https://doi.org/10.46743/2160-3715/2017.2674

Atkinson, J. (2002). Four steps to analyse data from a case study method. *ACIS 2002 Proceedings*, *38*, 1–11. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1138&context=acis2002

Austin, J., Cameron, T., Glass, M., Kosko, K., Marsh, F., Abdelmagid, R., & Burge, P. (2009). First semester experiences of professionals transitioning to full-time doctoral study. *College Student Affairs Journal*, *27*(2), 194–214. https://files.eric.ed.gov/fulltext/EJ882663.pdf

Auty, M. (2015). Anatomy of an advanced persistent threat. *Network Security*, *2015*(4), 13–16. https://doi.org/10.1016/S1353-4858(15)30028-3

Ayala, R. A., Koch, T. F., & Messing, H. B. (2019). Understanding the prospect of success in professional training: An ethnography into the assessment of problem-based learning. *Ethnography and Education*, *14*(1), 65–83. https://doi.org/10.1080/17457823.2017.1388184

Azhagiri, M., Rajesh, A., & Karthik, S. (2017). A multi-perspective and multi-level analysis framework in network security situational awareness. *International Journal of Computer Networks and Communications Security*, *5*(4), 71–75. https://ijcncs.org/published/volume5/issue4/p1_5-4.pdf

Bach, C., & Alshammari, M. (2013). Defense mechanisms for computer-based information systems. *International Journal of Network Security & Its Applications*, *5*(5), 107–113. https://doi.org/10.5121/ijnsa.2013.5509

Bahtiyar, Ş. (2018). A flow based approach to detect advanced persistent threats in communication systems. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *22*(Special), 519–528. https://doi.org/10.19113/sdufbed.98173

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018, Sept. 24). *Insider threat: The human element of cyberrisk*. McKinsey Insights. https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk#

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs. *Journal of Organizational Change Management, 31*(4), 839–851. https://doi.org/10.1108/JOCM-03-2017-0044

Bakirtzis, G., Carter, B. T., Fleming, C. H., & Elks, C. R. (2017). *MISSION AWARE: Evidence-based, mission-centric cybersecurity analysis.* https://arxiv.org/pdf/1712.01448.pdf

Balco, P., Law, J., & Drahošová, M. (2017). Cloud market analysis from customer perspective. *Procedia Computer Science*, *109*, 1022–1027. https://doi.org/10.1016/j.procs.2017.05.375

Bamakan, S. M. H., & Dehghanimohammadabadi, M. (2015). A weighted Monte Carlo simulation approach to risk assessment of information security management system. *International Journal of Enterprise Information Systems*, *11*(4), 63–78. https://doi.org/10.4018/IJEIS.2015100103

Bandler, J. (2018, July 1). Preparing today for tomorrow's attack: A cybersecurity expert details how to prepare for and plan against a cyberattack. *ABA Journal*, *104*(7), 30. https://www.abajournal.com/magazine/article/prepare_plan_against_cyberattack

Barnes, I. A. (2018). *Implementation of active cyber defense measures: The need for an international accord to address disputes*. Naval Postgraduate School (U.S.). Center for Homeland Defense and Security. https://www.hsdl.org/?abstract&did=821423

Basken, P. (2017, February 26). Cybersecurity, rising: Working to meet a national shortage of computer-safety personnel, colleges find customers and complications. *The Chronicle of Higher Education*, *63*(26), B18+. https://www.chronicle.com/article/cybersecurity-rising/

Behnsen, W., & Faber, E. (2012). *Secure ICT service provisioning for cloud, mobile and beyond: A workable architectural approach balancing between buyers and providers*. Springer.

Belotto, M. J. (2018). Data analysis methods for qualitative research: Managing the challenges of coding, interrater reliability, and thematic analysis. *The Qualitative Report*, *23*(11), 2622–2633. https://doi.org/10.46743/2160-3715/2018.3492

Bernardo, D. V. (2015). Clear and present danger: Interventive and retaliatory approaches to cyber threats. *Applied Computing and Informatics*, *11*(2), 144–157. https://doi.org/10.1016/j.aci.2014.11.002

Biernacki, P., & Waldorf, D. (2016). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological Methods & Research*, *10*(2), 141–163. https://doi.org/10.1177/004912418101000205

Bitektine, A. (2008). Prospective case study design: Qualitative method for deductive theory testing. *Organizational Research Methods*, *11*(1), 160–180. https://doi.org/10.1177/1094428106292900

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Boonstra, A., Eseryel, U. Y., & van Offenbeek, M. A. G. (2018). Stakeholders' enactment of competing logics in IT governance: Polarization, compromise or synthesis? *European Journal of Information Systems*, *27*(4), 415–433. https://doi.org/10.1057/s41303-017-0055-0

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information and Computer Security*, *23*(3), 317–332. https://doi.org/10.1108/ICS-09-2014-0064

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Brasington, H., & Park, M. (2016). Cybersecurity and ports: Vulnerabilities, consequences and preparation. *Ausmarine*, *38*(4), 23–24.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://www.tandfonline.com/doi/abs/10.1191/1478088706QP063OA

Bruce, A., Beuthin, R., Sheilds, L., Molzahn, A., & Schick-Makaroff, K. (2016). Narrative research evolving: Evolving through narrative research. *International Journal of Qualitative Methods*, *15*(1), 1–4. https://doi.org/10.1177/1609406916659292

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2018). On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, *15*(1), 20–45. https://doi.org/10.1002/jip.1482

Byres, E. J. (2014). Defense-in-depth: Reliable security to thwart cyber-attacks. *Pipeline and Gas Journal*, *241*(2), 58. https://www.pgjonline.com

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5–10. https://doi.org/10.1016/S1361-3723(13)70062-9

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security*, *2016*(6), 8–14. https://doi.org/10.1016/S1361-3723(15)30046-4

Cameron, E. A., & Marcum, T. M. (2019). Why business schools must incorporate cybersecurity into the business curriculum: Preparing the next generation for success. *Journal of Higher Education Theory and Practice*, *19*(4), 25–33. https://doi.org/10.33423/jhetp.v19i4.2199

Cameron, R., & Molina-Azorin, J. F. (2011). The acceptance of mixed methods in business and management research. *International Journal of Organizational Analysis*, *19*, 256–271. https://doi.org/10.1108/19348831111149204

Carless, D., & Douglas, K. (2017). Narrative research. *The Journal of Positive Psychology: Qualitative Positive Psychology*, *12*(3), 307–308. https://doi.org/10.1080/17439760.2016.1262611

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Caviglione, L., Gaggero, M., Lalande, J., Mazurczyk, W., & Urbanski, M. (2016). Seeing the unseen: Revealing mobile malware hidden communications via energy consumption and artificial intelligence. *IEEE Transactions on Information Forensics and Security*, *11*(4), 799–810. https://doi.org/10.1109/TIFS.2015.2510825

Chang, J. M., Ho, P.-C., & Chang, T.-C. (2014). Securing BYOD. *IT Professional*, *16*(5), 9–11. https://doi.org/10.1109/MITP.2014.76

Chapman, J. M. H. (2014). *Researcher as participant: Safeguarding against bias in a qualitative case study*. Sage.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Chen, Y. V., Qian, Z. Q., & Lei, W. T. (2016). Designing a situational awareness information display: Adopting an affordance-based framework to amplify user experience in environmental interaction design. *Informatics*, *3*(2), 6. https://doi.org/10.3390/informatics3020006

Chenail, R. J. (2012a). Conducting qualitative data analysis: Qualitative data analysis as a metaphoric process. *The Qualitative Report*, *17*(1), 248–253. https://nsuworks.nova.edu/tqr/vol17/iss1/13

Chenail, R. J. (2012b). Conducting qualitative data analysis: Reading line-by-line, but analyzing by meaningful qualitative units. *The Qualitative Report, 17*(1), 266–269. https://files.eric.ed.gov/fulltext/EJ973045.pdf

Cho, J.-H., & Ben-Asher, N. (2018). Cyber defense in breadth: Modeling and analysis of integrated defense systems. *The Journal of Defense Modeling and Simulation*, *15*(2), 147–160. https://doi.org/10.1177/1548512917699725

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

Chun Tie, Y., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine*, *1–8*, 205031211882292. https://doi.org/10.1177/2050312118822927

Clarke, K., Levy, Y., Dringus, L., & Brown, S. (2019). How workplace satisfaction affects insider threat detection as a vital variable for the mitigation of malicious cyber insiders. *Online Journal of Applied Knowledge Management*, *7*(1), 40–52. https://doi.org/10.36965/OJAKM.2019.7(1)40-52

Clay, P. (2015). A modern threat response framework. *Network Security*, *2015*(4), 5–10. https://doi.org/10.1016/S1353-4858(15)30026-X

Cleghorn, L. (2013). Network defense methodology: A comparison of defense in depth and defense in breadth. *Journal of Information Security*, *4*(3), 144–149. https://doi.org/10.4236/jis.2013.43017

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods*, *13*(1), 88–103. https:/doi.org/10.1177/160940691401300134

Condit, C. M., Korngiebel, D. M., Pfeifer, L., Renz, A. D., Bowen, D. J., Kaufman, D., Kollar, L. M. M., & Edwards, K. L. (2015). What should be the character of the researcher-participant relationship? Views of participants in a long-standing cancer genetic registry. *IRB*, *37*(4), 1–10. https://www.jstor.org/stable/24574939

Conti, G., & Fanelli, R. (2019). How could they not: Thinking like a state cyber threat actor. *The Cyber Defense Review*, *4*(2), 49–64. https://doi.org/10.2307/26843892

Conway, J. M., Jako, R. A., & Goodman, D. F. (1995). A meta- analysis of interrater and internal consistency reliability of selection interviews. *Journal of Applied Psychology*, *80*(5), 565–579. https://doi.org/10.1037/0021-9010.80.5.565

Coppel, C. (2016, November 1). The cybersecurity crisis: Many professionals believe cybersecurity skills are lacking in their organizations. *TD Magazine*, *70*(11), 14. https://www.td.org/magazines/td-magazine/the-cybersecurity-crisis

Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage.

Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. *Decision Analysis*, *17*(4), 356–374. https://doi.org/10.1287/deca.2020.0418

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Sage.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Sage.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A. J., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, *11*(1), 100. https://doi.org/10.1186/1471-2288-11-100

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity framework*. Department of Homeland Security. https://www.us-cert.gov/resources/cybersecurity-framework

Dai, J., Chen, C., & Li, Y. (2019). A backdoor attack against LSTM-based text classification systems. *IEEE Access*, *7*, 138872–138878. https://doi.org/10.1109/ACCESS.2019.2941376

Davis, P. K. (2014). Deterrence, influence, cyber attack, and cyberwar. *New York University Journal of International Law and Politics*, *47*(2), 327–355. https://www.nyujilp.org

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*, *35*(2), 60–67. https://doi.org/10.1177/0266382118773624

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management*, *20*(3), 107–121. https://doi.org/10.1007/s10799-018-00297-3

De Chaves, S. A., Uriarte, R. B., & Westphall, C. B. (2011). Toward an architecture for monitoring private clouds. *IEEE Communications Magazine*, *49*(12), 130–137. https://doi.org/10.1109/MCOM.2011.6094017

Demchenko, Y., Zhao, Z., Grosso, P., Wibisono, A., & De Laat, C. (2012, December). Addressing big data challenges for scientific data infrastructure. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference* (pp. 614–617). IEEE. https://www.uazone.org/demch/papers /cloudcom2012poster-bigdata-infra-v03.pdf

Denning, D. E., & Strawser, B. J. (2014). *Active cyber defense: Applying air defense to the cyber domain*. The National Postgraduate School (NPS) Institutional Archive.

Denning, P. J., & Denning, D. E. (2016). Cybersecurity is harder than building bridges. *American Scientist*, *104*(3), 155. https://doi.org/10.1511/2016.120.155

Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Computer Fraud & Security*, *2016*(10), 5–8. https://doi.org/10.1016/S1361-3723(16)30079-3

Devos, J., & van de Ginste, K. (2015). Towards a theoretical foundation of IT governance—The COBIT 5 case. *Electronic Journal of Information Systems Evaluation*, *18*(2), 95–103. https://biblio.ugent.be/publication/6966348/file/6966361.pdf

Dewar, R. S. (2014, June). The “triptych of cyber security”: A classification of active cyber defence. *2014 6th International Conference on Cyber Conflict*, 7–21. https://doi.org/10.1109/cycon.2014.6916392

Dodgson, J. E. (2019). Reflexivity in qualitative research. *Journal of Human Lactation, 35*(2), 220–222. https://doi.org/10.1177/0890334419830990

Dominitz, E. J. (2017). To err is human; to insure, divine: Shouldn’t cyber insurance cover data breach losses arising [in whole or in part] from negligence? *The Brief, 46*(4), 32–37. https://www.americanbar.org

Donalds, C., & Osei-Bryson, K. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior, 92*, 403–418. https://doi.org/10.1016/j.chb.2018.11.039

Dressler, J., Bowen, C. L., Moody, W., & Koepke, J. (2014). Operational data classes for establishing situational awareness in cyberspace. *2014 6th International Conference on Cyber Conflict*, 175–186. https://doi.org/10.1109/CYCON.2014.6916402

Elliott, V. (2018). Thinking about the coding process in qualitative data analysis. *The Qualitative Report, 23*(11), 2850–2861. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=3560&context=tqr

Er Amandeep, S. W. (2017). Security vulnerability in mobile cloud computing (MCC). *International Journal of Advanced Research in Computer Science*, *8*(4). https://doi.org/10.26483/ijarcs.v8i4

Erbacher, R. F., Frincke, D. A., Wong, P. C., Moody, S., & Fink, G. (2010). A multi-phase network situational awareness cognitive task analysis. *Information Visualization*, *9*(3), 204–219. https://doi.org/10.1057/ivs.2010.5

Experian. (2017). *Providing more insight into the small business owner: A study by Experian's Business Information Solutions* [White paper]. https://www.experian.com/whitepapers/BOLStudy_Experian.pdf

Fawaz, K., & Shin, K. G. (2019). Security and privacy in the Internet of Things. *Computer*, *52*(4), 40–49. https://doi.org/10.1109/MC.2018.2888765

FBI News. (2015, January 20). *Ransomware on the rise. FBI and partners working to combat this cyber threat*. FBI.gov. https://www.fbi.gov/news/stories/ransomware-on-the-rise

FBI News. (2020, February 11). *2019 internet crime report*. FBI.gov. https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

Federal Bureau of Investigation, Internet Crime Complaint Center. (2018). *2018 internet crime report*. FBI.gov. https://pdf.ic3.gov/2018_IC3Report.pdf

Federal Bureau of Investigation. (2018, October 12). *Scams and safety: Common scams and crimes: Internet fraud*. FBI.gov. https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, 80–92. https://doi.org/10.1177/160940690600500107

Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk assessment uncertainties in cybersecurity investments. *Games*, *9*(2), 34. https://doi.org/10.3390/g9020034

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal of Business Continuity & Emergency Planning*, *11*(2), 163–173. https://www.ingentaconnect.com/content/hsp/jbcep/2017/00000011/00000002/art00006

Fowler, F. J. (2014). *Survey research methods*. Sage.

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology & Health*, *25*(10), 1229–1245. https://doi.org/10.1080/08870440903194015

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Friedberg, I., Skopik, F., & Fiedler, R. (2015). Cyber situational awareness through network anomaly detection: State of the art and new approaches. *E & i Elektrotechnik Und Informationstechnik*, *132*(2), 101–105. https://doi.org/10.1007/s00502-015-0287-4

Furnell, S., & Dowling, S. (2019). Cyber crime: A portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, *5*(1), 13–26. https://doi.org/10.1108/JCRPP-07-2018-0021

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408–1416. https://nsuworks.nova.edu/tqr/vol20/iss9/3/

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348. https://doi.org/10.1080/09636412.2015.1038188

Ge, M., Hong, J. B., Yusuf, S. E., & Kim, D. S. (2018). Proactive defense mechanisms for the software-defined internet of things with non-patchable vulnerabilities. *Future Generation Computer Systems, 78*, 568–582. https://doi.org/10.1016/j.future.2017.07.008

German, P. (2018). Fixing the cyber security skills shortage. *Database and Network Journal*, *48*(1), 21. https://www.pbctoday.co.uk/news/hr-skills-news/cyber-security-skills-shortage/39410/

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. *Procedia Computer Science*, *57*, 710–715. https://doi.org/10.1016/j.procs.2015.07.458

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

Granåsen, M., & Andersson, D. (2016). Measuring team effectiveness in cyber-defense exercises: A cross-disciplinary case study. *Cognition, Technology & Work*, *18*(1), 121–143. https://doi.org/10.1007/s10111-015-0350-2

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Hadji-Janev, M., & Bogdanoski, M. (2017). Swarming-based cyber defence under the framework of collective security. *Security Journal*, *30*(1), 39–59. https://doi.org/10.1057/sj.2016.7

Hammer, G. (2013). *Governance of enterprise IT based on COBIT®5: A management guide*. IT Governance Publishing. https://www.jstor.org/stable/j.ctt7zsxfv

Hammersley, M. (2006). Ethnography: Problems and prospects. *Ethnography and Education*, *1*(1), 3–14. https://doi.org/10.1080/17457820500512697

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

Hawkins, N. (2017). Why communication is vital during a cyber-attack. *Network Security*, *2017*(3), 12–14. https://doi.org/10.1016/S1353-4858(17)30028-4

Hayden, E. C. (2015). Cybercrime fight targets user error. *Nature*, *518*(7539), 282–283. https://doi.org/10.1038/518282a

Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons*, *61*(5), 689–697. https://doi.org/10.1016/j.bushor.2018.02.001

He, W., Zhang, Z., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Heikkilä, M., Rättyä, A., Pieskä, S., & Jämsä, J. (2016, June). Security challenges in small-and medium-sized manufacturing enterprises. *Proceedings: 2016 International Symposium on Small-Scale Intelligent Manufacturing Systems (SIMS)*, 25–30. IEEE. https://doi.org/10.1109/sims.2016.7802895

Herbane, B. (2019). Rethinking organizational resilience and strategic renewal in SMEs. *Entrepreneurship & Regional Development*, *31*(5–6), 476–495. https://doi.org/10.1080/08985626.2018.1541594

Hewes, C. A., Jr. (2016, Spring). Threat and challenges of cyber-crime and the response. *SAM Advanced Management Journal*, *81*(2), 4+. https://www.thefreelibrary.com/Threat+and+challenges+of+cyber-crime+and+the+response.-a0460761246

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT. *ACM Computing Surveys*, *52*(2), 1–40. https://doi.org/10.1145/3303771

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: Trends and challenges. *IEEE Communications Surveys & Tutorials*, *17*(4), 2242–2270. https://doi.org/10.1109/COMST.2015.2457491

Hu, F., Lu, Y., Vasilakos, A. V., Hao, Q., Ma, R., Patil, Y., Zhang, T., Lu, J., Li, X., & Xiong, N. N. (2016). Robust cyber–physical systems: Concept, models, and implementation. *Future Generation Computer Systems*, *56*, 449–475. https://doi.org/10.1016/j.future.2015.06.006

Hu, H., Wu, J., Wang, Z., & Cheng, G. (2018). Mimic defense: A designed-in cybersecurity defense framework. *IET Information Security*, *12*(3), 226–237. https://doi.org/10.1049/iet-ifs.2017.0086

Huang, L., & Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems. *Computers & Security*, *89*, 101660. https://doi.org/10.1016/j.cose.2019.101660

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security: A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

Information Systems Audit and Control Association. (2012a). *COBIT 5: A business framework for the governance and management of enterprise IT*. Abe Books.

Information Systems Audit and Control Association. (2012b). *COBIT 5 for information security*. Abe Books.

Information Systems Audit and Control Association. (2013). *Transforming cybersecurity: Using COBIT 5*. Abe Books.

Information Systems Audit and Control Association. (2019a). *ISACA's state of cybersecurity 2019 survey: Retaining qualified cybersecurity professionals increasingly challenging for organizations*. https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/isacas-state-of-cybersecurity-2019-survey-retaining-qualified-cybersecurity-professionals

Information Systems Audit and Control Association. (2019b). *State of cybersecurity 2019, part 2: Current trends in attacks, awareness and governance* [White paper]. https://www.isaca.org/boIokstore/state-of-cybersecurity-2019/whpsc192

Ioannidis, C., Pym, D., Williams, J., & Gheyas, I. (2019). Resilience in information stewardship. *European Journal of Operational Research, 274*(2), 638–653. https://doi.org/10.1016/j.ejor.2018.10.020

Jackson, S., Vanteeva, N., & Fearon, C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from U.S. firms. *Journal of the Association for Information Science and Technology*, *70*(11), 1277–1289. https://doi.org/10.1002/asi.24188

Jajodia, S., Subrahmanian, V. S., Swarup, V., & Wang, C. (Eds.). (2016). *Cyber deception: Building the scientific foundation* (1st ed.). Springer International Publishing. https://doi.org/10.1007/978-3-319-32699-3

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

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, *5*(4), 87–88. https://doi.org/10.4103/0976-0105.141942

Jarsa, V., & Christianto, K. (2018). IT governance audit with COBIT 5 framework on DSS domain. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *3*(4), 279–286. https://doi.org/10.22219/kinetik.v3i4.665

Jones, K. A., Beecroft, N. J., & Patterson, E. S. (2014). Towards computer-assisted coding: A case study of "charge by documentation" software at an endoscopy clinic. *Health Policy and Technology*, *3*(3), 208–214. https://doi.org/10.1016/j.hlpt.2014.05.002

Jugdev, K. (2019). Governance and governmentality for projects: Enablers, practices, and consequences. *International Journal of Managing Projects in Business, 13*(1), 228–234. https://doi.org/10.1108/IJMPB-03-2019-278

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kachgal, J. A. (2015). The synergy needed for business resilience. *Journal of Business Continuity & Emergency Planning*, *9*(1), 10–17. https://www.henrystewartpublications.com/jbcep

Kaila, U. (2018). Information security best practices: First steps for startups and SMEs. *Technology Innovation Management Review*, *8*(11), 32–42. https://doi.org/10.22215/timreview/1198

Karoui, K. (2016). Security novel risk assessment framework based on reversible metrics: A case study of DDoS attacks on an E-commerce web server. *International Journal of Network Management*, *26*(6), 553–578. https://doi.org/10.1002/nem.1956

Kaspersky Lab. (2017). *Cyber security for business—Counting the costs, finding the value* [White paper]. https://media.kaspersky.com/pdf/b2b/kaspersky-cybersecurity-for-business-roi-whitepaper.pdf

Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed denial of service attacks: A threat or challenge. *New Review of Information Networking*, *24*(1), 31–103. https://doi.org/10.1080/13614576.2019.1611468

Kaušpadienė, L., Ramanauskaitė, S., & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*, *25*(5), 979–997. https://doi.org/10.3846/tede.2019.10298

Keller, T., & Alsdorf, K. L. (2014). *Every good endeavor: Connecting your work to God's work.* Dutton.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14. https://doi.org/10.1016/S1361-3723(19)30085

Kennedy, S. E. (2016). The pathway to security—mitigating user negligence. *Information and Computer Security*, *24*(3), 255–264. https://doi.org/10.1108/ICS-10-2014-0065

Khera, M. (2017). Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. *Journal of Diabetes Science and Technology*, *11*(2), 207–212. https://doi.org/10.1177/1932296816677576

Khosroshahy, M., Mehmet Ali, M. K., & Qiu, D. (2013). The SIC botnet lifecycle model: A step beyond traditional epidemiological models. *Computer Networks, 57*(2), 404–421. https://doi.org/10.1016/j.comnet.2012.07.020

Kim, L. (2018). Cybersecurity matters. *Nursing Management*, *49*, 16–22. https://doi.org/10.1097/01.NUMA.0000529921.97762.be

Korba, A. A., Nafaa, M., & Ghanemi, S. (2016). An efficient intrusion detection and prevention framework for ad hoc networks. *Information and Computer Security*, *24*(4), 298–325. https://doi.org/10.1108/ICS-08-2015-0034

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, *24*(1-3), 72–77. https://doi.org/10.1080/19393555.2015.1051676

Král, P., & Králová, V. (2016). Approaches to changing organizational structure: The effect of drivers and communication. *Journal of Business Research*, *69*(11), 5169–5174. https://doi.org/10.1016/j.jbusres.2016.04.099

Krathwohl, D. R. (2009). *Methods of educational and social science research: The logic of methods*. Waveland.

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology* (2nd ed.). Sage.

Krishan, R. (2018). Corporate solutions to minimize expenses from cyber security attacks in the United States. *Journal of Internet Law*, *21*(11), 16–19.

Ktari, R. (2010). Coding choices for thematic text analysis: A comparison of manual text coding and computer-assisted coding. *International Journal of the Humanities*, *8*(3), 1–11. https://doi.org/10.18848/1447-9508/CGP/v08i03/42881

Kure, H., Islam, S., & Razzaque, M. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898

Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications*, *4*(4), 332–340. https://doi.org/10.1049/iet-cps.2018.5079

Lai, Y.-P., & Wu, W.-F. (2015). The defense in-depth approach to the protection for browsing users against drive-by cache attacks. *Security and Communication Networks*, *8*(7), 1422–1430. https://doi.org/10.1002/sec.1091

Lee, C., Song, B., & Park, Y. (2015). An instrument for scenario-based technology roadmapping: How to assess the impacts of future changes on organisational plans. *Technological Forecasting & Social Change*, *90*(Part A), 285–301. https://doi.org/10.1016/j.techfore.2013.12.020

Lee, J., Kim, J.-H., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access*, *7*, 165607–165626. https://doi.org/10.1109/ACCESS.2019.2953095

Lee, R. M. (2015). *The sliding scale of cyber security* [White paper]. SANS Institute: Information Security Reading Room. https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design.* Pearson.

Lenders, V., Tanner, A., & Blarer, A. (2015). Gaining an edge in cyberspace with advanced situational awareness. *IEEE Security & Privacy*, *13*(2), 65–74. https://doi.org/10.1109/MSP.2015.30

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

Lonsdale, D. J. (2018). Warfighting for cyber deterrence: A strategic and moral imperative. *Philosophy & Technology*, *31*(3), 409–429. https://doi.org/10.1007/s13347-017-0252-8

Lukosch, S., Lukosch, H., Datcu, D., & Cidota, M. (2015). Providing information on the spot: Using augmented reality for situational awareness in the security domain. *Computer Supported Cooperative Work*, *24*(6), 613–664. https://doi.org/10.1007/s10606-015-9235-4

Magnusson, E., & Marecek, J. (2015). *Doing interview-based qualitative research: A learner's guide*. Cambridge University Press.

Majhi, S. K., & Dhal, S. K. (2016). A study on security vulnerability on cloud platforms. *Procedia Computer Science*, *78*, 55–60. https://doi.org/10.1016/j.procs.2016.02.010

Major BEC gang targets top executives. (2018). *Computer Fraud & Security*, *2018*(12), 19. https://doi.org/10.1016/S1361-3723(18)30121-0

Malatji, M., von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

Mansfield-Devine, S. (2016a). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8–17. https://doi.org/10.1016/S1353-4858(16)30096-4

Mansfield-Devine, S. (2016b). The imitation game: How business email compromise scams are robbing organisations. *Computer Fraud & Security*, *2016*(11), 5–10. https://doi.org/10.1016/S1361-3723(16)30089-6

Marquardt, N. (2019). Situation awareness, human error, and organizational learning in sociotechnical systems. *Human Factors and Ergonomics in Manufacturing & Service Industries*, *29*(4), 327–339. https://doi.org/10.1002/hfm.20790

Marrelli, A. F. (2007). Collecting data through case studies. *Performance Improvement*, *46*(7), 39–44. https://doi.org/10.1002/pfi.148

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

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research*, *11*(3), 8. https://doi.org/10.17169/fqs-11.3.1428

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McKim, C. A. (2017). The value of mixed methods research: A mixed methods study. *Journal of Mixed Methods Research*, *11*(2), 202–222. https://doi.org/10.1177/1558689815607096

Meyers, A. (2018). Not your fairy-tale prince: The Nigerian business email compromise threat. *Computer Fraud & Security*, *2018*(8), 14–16. https://doi.org/10.1016/S1361-3723(18)30076-9

Mihas, P. (2019). *Learn to build a codebook for a generic qualitative study*. SAGE Publications, Limited.

Mikhed, V., & Vogan, M. (2018). How data breaches affect consumer credit. *Journal of Banking and Finance, 88,* 192–207. https://doi.org/10.1016/j.jbankfin.2017.12.002

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional, 14*(5), 53–55. https://doi.org/10.1109/MITP.2012.93

Mills, A. J., Durepos, G., & Wiebe, E. (Eds.). (2010). *Encyclopedia of case study research* (Vols. I–II). Sage. https://doi.org/10.4135/9781412957397

Miraglia, A., & Casenove, M. (2016). Fight fire with fire: The ultimate active defence. *Information and Computer Security, 24*(3), 288–296. https://doi.org/10.1108/ICS-01-2015-0004

Miranda, M. J. A. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review, 14*(2), 5–10, 56. http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., & Barbaray, R. (2018). The industrial management of SMEs in the era of Industry 4.0. *International Journal of Production Research, 56*(3), 1118–1136. https://doi.org/10.1080/00207543.2017.1372647

Moghimi, M., & Varjani, A. Y. (2016). New rule-based phishing detection method. *Expert Systems with Applications, 53,* 231–242. https://doi.org/10.1016/j.eswa.2016.01.028

Morse, E. A., Raval, V., & Wingender, J. R. (2018). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. *Business Lawyer, 73*(1), 1–34. https://qa.americanbar.org/content/dam/aba/publications/business_lawyer/2018/73_1/article-cybersecurity-201801.pdf

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, *140*(4), 70–92. https://doi.org/10.1162/DAED_a_00116

Musman, S., & Turner, A. (2018). A game theoretic approach to cyber security risk management. *The Journal of Defense Modeling and Simulation*, *15*(2), 127–146. https://doi.org/10.1177/1548512917699724

Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588–600. https://doi.org/10.1016/j.ejor.2016.12.034

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Naumes, W., & Naumes, M. J. (2012). *The art & craft of case writing* (3rd ed.). M. E. Sharpe.

Neal, P., & Ilsever, J. (2016). Protecting information: Active cyber defence for the business entity: A prerequisite corporate policy. *Academy of Strategic Management Journal*, *15*(2), 15–35.

Nebbione, G., & Calzarossa, M. C. (2020). Security of IoT application layer protocols: Challenges and findings. *Future Internet*, *12*(3), 55. https://doi.org/10.3390/fi12030055

Newmeyer, N. (2015). Changing the future of cyber-situational awareness. *Journal of Information Warfare*, *14*(2), 31–40, IV. https://www.jstor.org/stable/26487492

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ICS-07-2016-0061

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, *49*, 208–216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

Nikolopoulos, S. D., & Polenakis, I. (2017). Preventing malware pandemics in mobile devices by establishing response-time bounds. *Journal of Information Security and Applications*, *37*, 1–14. https://doi.org/10.1016/j.jisa.2017.09.002

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*(2), 34–35. https://doi.org/10.1136/eb-2015-102054

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Norman, D. (2017). Design, business models, and human–technology teamwork: As automation and artificial intelligence technologies develop, we need to think less about human–machine interfaces and more about human-machine teamwork. *Research-Technology Management: Innovation Management—The State of the Art*, *60*(1), 26–30. https://doi.org/10.1080/08956308.2017.1255051

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*, 1–13. https://doi.org/10.1177/1609406917733847

Nyre-Yu, M., Gutzwiller, R. S., & Caldwell, B. S. (2019). Observing cyber security incident response: Qualitative themes from field research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 437–441. https://doi.org/10.1177/1071181319631016

Okamoto, T., & Tarao, M. (2018). An artificial immunity-enhancing module for internet servers against cyberattacks. *Artificial Life and Robotics*, *23*(3), 292–297. https://doi.org/10.1007/s10015-018-0426-1

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

O'Reilly, M., & Parker, N. (2013). "Unsatisfactory Saturation": A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*(2), 190–197. https://doi.org/10.1177/1468794112446106

Osawa, J. (2017). The escalation of state sponsored cyberattack and national cyber security affairs: Is strategic cyber deterrence the key to solving the problem? *Asia-Pacific Review*, *24*(2), 113–131. https://doi.org/10.1080/13439006.2017.1406703

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change*, *70*(4), 397–420. https://doi.org/10.1007/s10611-018-9774-y

Park, M., Han, J., Oh, H., & Lee, K. (2019). Threat assessment for android environment with connectivity to IoT devices from the perspective of situational awareness. *Wireless Communications and Mobile Computing*, *2019*, 1–14. https://doi.org/10.1155/2019/5121054

Patton, E., & Appelbaum, S. H. (2003). The case for case studies in management research. *Management Research News*, *26*(5), 60–71. https://doi.org/10.1108/01409170310783484

Paul, J. A., & Wang, X. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, *122*, 113069. https://doi.org/10.1016/j.dss.2019.05.009

Petruzzelli, E., & Sharma, N. (2019). Closing the gaps in cybersecurity. *Chemical Engineering Progress*, *115*(11), 35–39.

Pharris, L. J. (2019). *Social engineering: How U.S. businesses strengthen the weakest link against cybersecurity threats* (2159) [Doctoral dissertation, Liberty University]. https://digitalcommons.liberty.edu/doctoral/2159

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224–232. https://www.ingentaconnect.com/content/hsp/jbcep/2019/00000012/00000003/art00004

Piantanida, M., & Garman, N. B. (1999). *The qualitative dissertation: A guide for students and faculty*. Corwin Press.

Poulsen, S. B., & Thøgersen, U. (2011). Embodied design thinking: A phenomenological perspective. *CoDesign*, *7*(1), 29–44. https://doi.org/10.1080/15710882.2011.563313

Pöyhönen, J., Nuojua, V., Lehto, M., & Rajamäki, J. (2019). Cyber situational awareness and information sharing in critical infrastructure organizations. *Information & Security*, *43*(2), 236–256. https://doi.org/10.11610/isij.4318

Presher, A. (2015). Defense-in-depth cybersecurity: Multiple defenses to harden network infrastructures and better management of user access are defeating threats that can be physical, procedural, or electronic. *Design News*, *70*(9), 34.

Proof Point. (2019). *The human factor report 2019*. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, 887–909. https://doi.org/10.1016/j.future.2019.03.00

Qassim, Q. S., Jamil, N., Daud, M., Patel, A., & Norhamadi Ja'affar. (2019). A review of security assessment methodologies in industrial control systems. *Information and Computer Security*, *27*(1), 47–61. https://doi.org/10.1108/ICS-04-2018-0048

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. https://doi.org/10.1108/K-12-2014-0283

Rai, S., & Chukwuma, P. (2016). Must-have controls for SMBs: Five controls can help small and mid-sized businesses protect themselves against cyber breaches. *Internal Auditor*, *73*(6), 16.

Rai, S., & Chukwuma, P. (2019). Does your organization need cyber monitoring 24x7x365? *EDPACS: The EDP Audit, Control, and Security Newsletter*, *60*(5), 6–9. https://doi.org/10.1080/07366981.2019.1690187

Rajivan, P., & Cooke, N. J. (2018). Information-pooling bias in collaborative security incident correlation analysis. *Human Factors*, *60*(5), 626–639. https://doi.org/10.1177/0018720818769249

Ransbotham, S., Kiron, D., Gerbert, P., & Reeves, M. (2017, September 6). Reshaping business with artificial intelligence: Closing the gap between ambition and action. *MIT Sloan Management Review*, *59*(1). https://sloanreview.mit.edu/projects/reshaping-business-with-artificial-intelligence/

Rapuzzi, R., & Repetto, M. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. *Future Generation Computer Systems*, *85*, 235–249. https://doi.org/10.1016/j.future.2018.04.007

Rass, S., Konig, S., & Schauer, S. (2017). Defending against advanced persistent threats using game-theory. *PLoS ONE*, *12*(1), e0168675. https://doi.org/10.1371/journal.pone.0168675

Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity: Building a successful defense program. *Frontiers of Health Services Management*, *35*(1), 13–22. https://doi.org/10.1097/HAP.0000000000000037

Recent cyberattack raises alarm. (2020, April). *Chemical Engineering Progress*, *116*(4), 7–9. https://www.aiche.org/resources/publications/cep/2020/april/cep-news-update/recent-cyberattack-raises-alarm

Resnik, D. B., & Finn, P. R. (2018). Ethics and phishing experiments. *Science and Engineering Ethics*, *24*(4), 1241–1252. https://doi.org/10.1007/s11948-017-9952-9

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: A call for cooperation in a new threat landscape. *Frontiers in Bioengineering and Biotechnology*, *7*, 99. https://doi.org/10.3389/fbioe.2019.00099

Riesco, R., & Villagra, V. A. (2019). Leveraging cyber threat intelligence for a dynamic risk framework. *International Journal of Information Security*, *18*(6), 715–739. https://doi.org/10.1007/s10207-019-00433-2

Rizov, V. (2018). Information sharing for cyber threats. *Information & Security: An International Journal, 39*(1), 43–50. https://doi.org/10.11610/isij.3904

Rubino, M., Vitolla, F., & Garzoni, A. (2017). The impact of an IT governance framework on the internal control environment. *Records Management Journal*, *27*(1), 19–41. https://doi.org/10.1108/RMJ-03-2016-0007

Ryan, N. J. (2018). Five kinds of cyber deterrence. *Philosophy & Technology, 31*(3), 331–338. https://doi.org/10.1007/s13347-016-0251-1

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications, 40,* 247–257. https://doi.org/10.1016/j.jisa.2017.11.001

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Safaei Pour, M., Bou-Harb, E., Varma, K., Neshenko, N., Pados, D. A., & Choo, K.-K. R. (2019). Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize internet-scale IoT probing campaigns. *Digital Investigation, 28*, S40–S49. https://doi.org/10.1016/j.diin.2019.01.014

Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using artificial neural networks. *Neurocomputing, 172*, 385–393. https://doi.org/10.1016/j.neucom.2015.04.101

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: A knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041

Sanders, J., & Spiering, S. (2016). How boards can have maximum impact on digital strategy: Before embarking on transformative strategic changes tied to digital technologies, companies should take steps to create more agile cultures. *Directors & Boards*, *40*(2), 50. https://www.directorsandboards.com/articles/singlehow-boards-can-have-maximum-impact-digital-strategy

Sarmiento, J. P., Hoberman, G., Jerath, M., & Jordao, G. F. (2016). Disaster risk management and business education: The case of small and medium enterprises. *Ad-Minister*, *28*, 73–90. https://doi.org/10.17230/ad-minister.28.4

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research methods for business students* (6th ed.). Pearson Education Limited.

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119–2126. https://doi.org/10.1111/risa.13309

Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information and Computer Security*, *24*(1), 73–92. https://doi.org/10.1108/ICS-03-2014-0020

Schiavone, S., Garg, L., & Summers, K. (2014). Ontology of information security in enterprises. *Electronic Journal of Information Systems Evaluation*, *17*(1), 71–87. https://issuu.com/academic-conferences.org/docs/ejise-volume17-issue1-article939?mode=a_p

Schneider, S., & Leyer, M. (2019). Me or information technology? Adoption of artificial intelligence in the delegation of personal strategic decisions. *Managerial and Decision Economics*, *40*(3), 223–231. https://doi.org/10.1002/mde.2982

Scholz, R. W., Czichos, R., Parycek, P., & Lampoltshammer, T. J. (2020). Organizational vulnerability of digital threats: A first validation of an assessment method. *European Journal of Operational Research*, *282*(2), 627–643. https://doi.org/10.1016/j.ejor.2019.09.020

Schoonenboom, J., & Johnson, R. B. (2017). How to construct a mixed methods research design. *KZfSS Kölner Zeitschrift Für Soziologie und Sozialpsychologie*, *69*(S2), 107–131. https://doi.org/10.1007/s11577-017-0454-1

Self, D. R., Self, T., Matuszek, T., & Schraeder, M. (2015). Improving organizational alignment by enhancing strategic thinking. *Development and Learning in Organizations*, *29*(1), 11–14. https://doi.org/10.1108/DLO-08-2013-0053

Setiawan, A. K., & Andry, J. F. (2019). Information technology governance performance measurement at national library using COBIT framework 5. *Jurnal Terapan Teknologi Informasi*, *3*(1), 53–63. https://doi.org/10.21460/jutei.2019.31.134

Severe shortage of cybersecurity professionals is a key risk to our nation's security. (2018, October–December). *CHIPS*. https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=10877

Shijo, P. V., & Salim, A. (2015). Integrated static and dynamic analysis for malware detection. *Procedia Computer Science*, *46*, 804–811. https://doi.org/10.1016/j.procs.2015.02.149

Shoemaker, D., Kohnke, A., & Sigler, K. (2019). What the profession of cybersecurity needs to know and do. *EDPACS: The EDP Audit, Control, and Security Newsletter*, *59*(2), 6–18. https://doi.org/10.1080/07366981.2019.1565106

Shree, A., Shree, D., & Ahlawat, S. (2017). A review on cryptography, attacks and cyber security. *International Journal of Advanced Research in Computer Science*, *8*(5), 239–242. https://doi.org/10.26483/ijarcs.v8i5.3283

Singh Kunwar, R., Sharma, P., & Ravi Kumar, K. V. (2018). Malware analysis of backdoor creator: FATRAT. *International Journal of Cyber-Security and Digital Forensics*, *7*(1), 72–79. https://doi.org/10.17781/P002362

Sinkovics, R. R., Penz, E., & Ghauri, P. N. (2008). Enhancing the trustworthiness of qualitative research in international business. *Management International Review*, *48*, 689–713. https://doi.org/10.1007/s11575-008-0103-z

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, *41*(3), 72–109. https://doi.org/10.1162/ISEC_a_00267

SMBs are a huge target for hackers. (2017). *Software World*, *48*(5), 26.

Smith, G. (2018). The intelligent solution: Automation, the skills shortage and cyber-security. *Computer Fraud & Security*, *2018*(8), 6–9. https://doi.org/10.1016/S1361-3723(18)30073-3

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), 42–60. https://doi.org/10.1108/JICES-02-2018-0010.

Sonenshein, S. (2010). We're changing—or are we? Untangling the role of progressive, regressive, and stability narratives during strategic change implementation. *The Academy of Management Journal*, *53*(3), 477–512. doi:10.5465/AMJ.2010.51467638

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, *75*, 49–62. https://doi.org/10.1016/j.dss.2015.04.011

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

Stake, R. E. (2010). *Qualitative research: Studying how things work*. Guilford Press.

Stanciu, V., & Tinca, A. (2017). Exploring cybercrime: Realities and challenges. *Journal of Accounting and Management Information Systems*, *16*(4), 610–632. https://doi.org/10.24818/jamis.2017.04009

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453–3495. https://doi.org/10.1109/COMST.2018.2855563

Strauss, A., & Corbin, J. M. (1997). *Grounded theory in practice*. Sage.

Strong cyber security helps businesses to grow. (2017). *Software World*, *48*(5), 25.

Succeeding with organizational change: A step-by-step approach. (2015). *Development and Learning in Organizations*, *29*(5), 19–21. https://doi.org/10.1108/DLO-03-2015-0017

Suen, L. W., Huang, H., & Lee, H. (2014). A comparison of convenience sampling and purposive sampling. *Hu Li Za Zhi*, *61*(3), 105–110. https://doi.org/10.6224/JN.61.3.105

Sunthonwutinun, W., & Chooprayoon, V. (2016). A proposed model for studying information technology governance, management, and services of an enterprise: An integrated framework of COBIT 5, ITIL®V3, and BSC. *International Journal of Computer Theory and Engineering*, *8*(2), 140–144. https://doi.org/10.7763/IJCTE.2016.V8.1033

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226–231. https://doi.org/10.4212/CJHP.V68I3.1456

Syed, M., & Nelson, S. C. (2015). Guidelines for establishing reliability when coding narrative data. *Emerging Adulthood*, *3*(6), 375–387. https://doi.org/10.1177/2167696815587648

Tagarev, T., Sharkov, G., & Stoianov, N. (2017). Cyber security and resilience of modern societies: A research management architecture. *Information & Security: An International Journal*, *38*, 93–108. https://doi.org/10.11610/isij.3807

Taitto, P., Nevmerzhitskaya, J., & Virag, C. (2018). Using holistic approach to developing cybersecurity simulation environments. *International Scientific Conference: eLearning & Software for Education*, *4*, 77–84. https://doi.org/10.12753/2066-026X-18-226

Tarao, M., & Okamoto, T. (2017). Performance evaluation of an immunity-enhancing module for server applications. *Procedia Computer Science*, *112*, 2165–2174. https://doi.org/10.1016/j.procs.2017.08.249

Timonen, V., Foley, G., & Conlon, C. (2018). Challenges when using grounded theory: A pragmatic introduction to doing GT research. *International Journal of Qualitative Methods*, *17*, 1–10. https://doi.org/10.1177/1609406918758086

Tolosa, J. (2015, October 5). Stopping the next SMB breach. *Computer Reseller News [UK]*, S10.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Trim, P. R. J., & Lee, Y. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003

Tripathi, S., & Nasina, J. (2017). Adoption of cloud computing in business: A multi-case approach to evaluate the fit-viability model (FVM). *International Journal of Business and Information*, *12*(1), 39–64. https://doi.org/10.6702/ijbi.2017.12.1.2

Tromble, R., & McGregor, S. C. (2019). You break it, you buy it: The naiveté of social engineering in tech—and how to fix it. *Political Communication*, *36*(2), 324–332. https://doi.org/10.1080/10584609.2019.1609860

Trotter, L., Harding, M., Mikusz, M., & Davies, N. (2018). IoT-enabled highway maintenance: Understanding emerging cybersecurity threats. *IEEE Pervasive Computing*, 17(3), 23–34. https://doi.org/10.1109/MPRV.2018.03367732

Tu, H., Xia, Y., Wu, J., & Zhou, X. (2019). Robustness assessment of cyber–physical systems with weak interdependency. *Physica A: Statistical Mechanics and its Applications*, *522*, 9–17. https://doi.org/10.1016/j.physa.2019.01.137

Tufford, L., & Newman, P. (2012). Bracketing in qualitative research. *Qualitative Social Work*, *11*(1), 80–96. https://doi.org/10.1177/1473325010368316

Ukil, M. I., & Akkas, M. A. (2017). Determining success factors for effective strategic change: Role of middle managers' strategic involvement. *Serbian Journal of Management*, *12*(1), 29–40. https://doi.org/10.5937/sjm12-11430

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

van Manen, M. (2016). *Phenomenology of practice: Meaning-giving methods in phenomenological research and writing*. Routledge.

van Wyk, J., & Rudman, R. (2019). COBIT 5 compliance: Best practices cognitive computing risk assessment and control checklist. *Meditari Accountancy Research*, *27*(5), 761–788. https://doi.org/10.1108/MEDAR-04-2018-0325

Vincent, A. (2017). State-sponsored hackers: The new normal for business. *Network Security*, *2017*(9), 10–12. https://doi.org/10.1016/S1353-4858(17)30113-7

Vincent, N. E. (2016, December). A holistic approach to IT risk: The COBIT framework can help auditors understand and address their organization's technology risks. *Internal Auditor*, *73*(6), 18. https://iaonline.theiia.org/2016/Pages/A-Holistic-Approach-to-IT-Risk.aspx

Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication Systems*, *73*(1), 3–25. https://doi.org/10.1007/s11235-019-00599-z

Visu, P., Lakshmanan, L., Murugananthan, V., & Cruz, M. V. (2019). Software-defined forensic framework for malware disaster management in Internet of Thing devices for extreme surveillance. *Computer Communications*, *147*, 14–20. https://doi.org/10.1016/j.comcom.2019.08.013

Vithayathil, J. (2018). Will cloud computing make the Information Technology (IT) department obsolete? *Information Systems Journal*, *28*(4), 634–649. https://doi.org/10.1111/isj.12151

Wagner, M. (2016). The hard truth about hardware in cyber-security: It's more important. *Network Security*, *2016*(12), 16–19. https://doi.org/10.1016/S1353-4858(16)30117-9

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*, 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Wani, A., & Revathi, S. (2020). Ransomware protection in IoT using software defined networking. *International Journal of Electrical and Computer Engineering*, *10*(3), 3166–3175. https://doi.org/10.11591/ijece.v10i3.pp3166-3175

Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, *89*(1), 1–12. https://doi.org/10.1140/epjb/e2015-60754-4

Whittemore, R., & Melkus, G. D. (2008). Designing a research study. *The Diabetes Educator*, *34*(2), 201–216. https://doi.org/10.1177/0145721708315678

Wilson, J. (2018). Scamming the scammers with their own tricks. *Computer Fraud & Security*, *2018*(9), 14–16. https://doi.org/10.1016/S1361-3723(18)30087-3

Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems*, *33*(2), 597–620. https://doi.org/10.1080/07421222.2016.1205934

Wolstenholme, E. F. (2017). Qualitative vs quantitative modelling: The evolving balance. *The Journal of the Operational Research Society*, *50*(4), 422–428. https://doi.org/10.1057/palgrave.jors.2600700

Xu, M., Hua, L., & Hua, L. (2019). Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, *23*(2), 220–249. https://doi.org/10.1080/10920277.2019.1566076

Xu, W., & Zammit, K. (2020). Applying thematic analysis to education: A hybrid approach to interpreting data in practitioner research. *International Journal of Qualitative Methods*, *19*, 1–9. https://doi.org/10.1177/1609406920918810

Yampolskiy, R. V., & Spellchecker, M. S. (2016). Artificial intelligence safety and cybersecurity: A timeline of AI failures. *arXiv.org*. https://arxiv.org/ftp/arxiv/papers/1610/1610.07997.pdf

Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big data and cloud computing: Innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13–53. https://doi.org/10.1080/17538947.2016.1239771

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

Zweighaft, D. (2017). Business email compromise and executive impersonation: Are financial institutions exposed? *Journal of Investment Compliance*, *18*(1), 1–7. https://doi.org/10.1108/JOIC-02-2017-0001

Appendix A: Interview Guide

Introduction

Thank you so much for taking part in this study and taking time for this interview. As I indicated in the initial email, my name is Binh Vo and I am a doctoral candidate at Liberty University. The purpose of my study is to investigate and explore the problem of the growing number of cyberattacks against U.S. businesses.

Before beginning the interview, I would like to inform you of a few details. The audio recording of this interview and its data, which I will transcribe for analysis, will be stored and protected securely at all times and I will be the only person who has access to it. Importantly, your identifying information will be extricated, as I understand that cybersecurity is a sensitive topic for discussing, regarding your job role and employing business. I will not use or share your identifying information under any circumstance, including your job title and employer. Your confidentiality is greatly assured! I also would like you to know that you are free to not answer any interview questions or decide to withdraw at any time. I will gladly answer any questions. Do you have any questions for me before we begin?

Interview Questions

1. From your working experience and cybersecurity perspective, what are cyber vulnerabilities that businesses often have?
    1. Where does [a specific type of cyber vulnerability] come from?
    2. What types of cyber vulnerability have you had experience with?
    3. How can business address cyber vulnerabilities with non-technical solutions?
    4. How can business address cyber vulnerabilities with technical mechanisms?
2. How are cyber vulnerabilities impacting business?

    1. Please answer if you can. What are the direct impacts of cyber vulnerabilities on your business and on a business organization that you know of?
    2. What is the non-monetary impact of cyber vulnerabilities on business?
3. What are barriers preventing business from solving their cyber vulnerabilities?
    1. What barriers do you think are the most challenging for business to solve to eliminate their vulnerabilities?
    2. What barriers do you think are difficult for business to overcome, even if they have the suitable financial budget?
4. What technical challenges are business having in improving their cybersecurity capability?
    1. How impactful are those technical challenges?
5. What organizational challenges are business having in strengthening their cybersecurity capability?
    1. How can business change their organizational elements to enhance cybersecurity?
    2. In what way should business change their policy and human resources for better cybersecurity?
6. What are cybersecurity mechanisms or tools that business can employ to better protect themselves?
    1. What cybersecurity technology do you think can boost cyber defense capability?
    2. What non-technical mechanisms should business employ for better cyber defense capability?

Closing Statement

Following this interview, I will transcribe this audio recording. When completed, I will send you a copy for reviewing and checking for accuracy. That will be an opportunity for you to provide clarification or additional details. Please feel free to contact me if you have any concerns. Do you have any questions or comments for me?

I greatly appreciate your participation in this study!