2023

Analyzing Small Business Strategies to Prevent External Cybersecurity Threats

Dr. Kevin E. Moore
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Kevin E. Moore

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jodine Burchell, Committee Chairperson, Information Technology Faculty
Dr. Bob Duhainy, Committee Member, Information Technology Faculty
Dr. Jon McKeeby, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2023

Abstract

Analyzing Small Business Strategies to Prevent External Cybersecurity Threats

by

Kevin E. Moore

MS, Walden University, 2016

MS, Purdue University Global, 2014

BS, Purdue University Global, 2013

AAS, Arkansas College of Technology, 1995

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2023

Abstract

Some small businesses’ cybersecurity analysts lack strategies to prevent their organizations from compromising personally identifiable information (PII) via external cybersecurity threats. Small business leaders are concerned, as they are the most targeted critical infrastructures in the United States and are a vital part of the economic system as data breaches threaten the viability of these organizations. Grounded in routine activity theory, the purpose of this pragmatic qualitative inquiry was to explore strategies small business organizations utilize to prevent external cybersecurity threats. The participants were nine cybersecurity analysts who utilized strategies to defend small businesses from external threats. Data were collected via online semistructured interviews and the National Institute of Standards and Technology documentation as well as analyzed thematically. Six major themes emerged: (a) applying standards regarding external threats, (b) evaluation of cybersecurity strategies and effectiveness, (c) consistent awareness of the external threat landscape, (d) assessing threat security posture, (e) measuring the ability to address risk and prevent attacks related to external threats, and (f) centralizing communication across departments to provide a holistic perspective on threats. A key recommendation for cybersecurity analysts is to employ moving the target defenses to prevent external cybersecurity threats. The implications for positive social change include the potential to provide small business cybersecurity analysts with additional strategies to effectively mitigate the compromise of customer PII, creating more resilient economic infrastructures while strengthening communities.

Analyzing Small Business Strategies to Prevent External Cybersecurity Threats

by

Kevin E. Moore

MS, Walden University, 2016

MS, Purdue University Global, 2014

BS, Purdue University Global, 2013

AAS, Arkansas College of Technology, 1995

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2023

Dedication

To my wife and children because without them, there is no I, as this academic journey would not have been possible. They allow me to focus my energy on completing the goals in my life, and for that, I am thankful. To my mother, who died suddenly on June 26th, 2022. She didn’t see me achieve this accomplishment; however, she told me she knew when I was a child that I would do great things. I believe being the first in my family to obtain a doctorate degree would qualify as one of them.

Acknowledgments

In retrospect, it was a dream of mine coming from humble beginnings to achieve my doctorate degree. It is a culmination of efforts that were both challenging and rewarding and reflected many individuals who were instrumental in sustaining my motivation to reach the finish line. I would like to thank Dr. Jodine Burchell for her everlasting positivity no matter the situation. Her guidance, support, and unique ability to take complex concepts and make them palatable were unmatched. I am grateful to have such a Chair. I would also like to thank my committee members, Dr. Bob Duhainy and Dr. Jon McKeeby. I would also like to thank the Program Director, Dr. Gail Miles. Lastly, I am grateful to all the gatekeepers and participants that played a role in this study. I am thankful for their thoughtfulness, time, and effort during this academic journey.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

Researchers have discovered a lack of resources in the small business cybersecurity domain (Almeida et al., 2018). Due to their small sizes, limited funds, and finite perceptions, small businesses often have access to a smaller pool of personnel and information technology (IT) resources than their larger corporate counterparts, creating a soft target perception amongst hackers, as reported by the National Institute of Standards and Technology (NIST, 2019a). Small businesses are an essential part of our nation's economic and cyber infrastructure as small businesses comprise 99.9% of all firms, 97.5% of exporting firms, and 47.3% of private-sector employees (Small Business Administration, 2019). Small businesses accounted for 64.9% of net new job creation from 2000 to 2018 while remaining the most prominent cyberattack targets. If not adequately mitigated, the consequences can ultimately render their organizations ill-prepared to remain operable (NIST, 2019a). Small businesses make up more than 97% of total businesses in the United States; they undoubtedly have a unique role in the cybersecurity ecosystem and provide insight into effective national security strategies for employees (Small Business Administration, 2019). Small businesses provide a conduit through which cybercriminals have access to larger corporations' supply chains within the 16 critical infrastructure sectors. If breached, they pose a considerable threat to national security (Department of Homeland Security, 2019).

Problem Statement

Securing electronic data within a small business computer system plagues these organizations even after 50 years of the onset of electronically stored data within a computer system. (Wirth, 2017). In the United States, in 2018, 70% of all data breaches targeted small businesses as they typically lacked the cybersecurity resources of larger organizations (Small Business Administration, 2018). The general IT problem is that many small business cybersecurity resources are inadequate to address potential cyberattacks. The specific IT problem is that some IT cybersecurity analysts of small businesses lack the strategies needed to prevent external cybersecurity threats.

Purpose Statement

The purpose of this pragmatic qualitative inquiry was to explore the strategies utilized by IT cybersecurity analysts of small businesses to prevent external cybersecurity threats. The targeted population to engage in this study were nine IT cybersecurity analysts of small businesses located in Texas. This study's population is appropriate because IT cybersecurity analysts institute the strategies and evaluate the resources to prevent cybersecurity threats. A small business is defined as having fewer than 500 employees (Small Business Administration, 2019). In this study, the positive social change implication includes the potential for decreasing the compromise of personally identifiable, confidential, or sensitive customer information. More so, enhancing cybersecurity strategies in small business organizations may provide a better allocation of finite resources to aid in formulating techniques and strategies that prevent theft of customers' personally identifiable information (PII).

Nature of the Study

The most appropriate method for this study is the qualitative method. The qualitative process involves exploring participants' viewpoints by utilizing open-ended questions while identifying themes from the responses, as Graebner et al. (2012) noted. I selected the qualitative methodology because the study called for an in-depth exploration of phenomena within the context of an identified incident. I also considered a quantitative method. Researchers apply the quantitative methodology to identify and investigate the impact of measurable variables to explain a phenomenon or outcome (Yin, 1981). Because this study did not involve quantifiable variables, the quantitative methodology would have been an inappropriate choice. Mixed-method was a third possibility; however, researchers combine data from both qualitative and quantitative datasets (Johnson & Onwuegbuzie, 2004). I did not have a numerical element in this study, so the mixed-methods approach would not have been a good choice. Because I am researching a phenomenon requiring in-depth exploration, the qualitative method was most appropriate for this study.

I selected a pragmatic qualitative research design for this study as it is appropriate for exploratory research. Positioning my study to remain in alignment with Patton's (2015) explanation of pragmatic inquiry as "seeking practical and useful insights to inform action" (p. 153), I asked participants in this exploratory study about their experiences in the prevention practices of cybersecurity analysts, precisely to determine and explore strategies utilized to prevent cybersecurity threats through the lens of nine cybersecurity analysts. This exploratory study was drafted to elicit responses that may provide a window into trends, tactics, practices, and less often utilized "moving the target defenses" (MTD) methods to inform mitigation techniques in the future. Shoring up small business resources to provide for job growth and further research to aid in protecting customer PII. The purpose of pragmatic qualitative research is to link theory with practice (Savin-Baden & Major, 2013). In pragmatic qualitative research, the intent is to present a complete description of a phenomenon within a specific context in a real-world setting, allowing a liberal amount of flexibility in methods and techniques applied to understanding a not yet understood phenomenon (Leedy & Ormrod, 2015). Because I was researching a phenomenon within small businesses, the pragmatic qualitative research design was most appropriate to research the problem. The phenomenological design explores several participants' lived experiences around a specific issue or phenomenon (Myers, 1997). Given that this study's aim was not to explore participants' behavioral and learned patterns, customs, or ways of life, the phenomenological design would have been inappropriate for this study. Snape et al. (2014) proposed that the Delphi technique utilizes a structured communication technique within a group to develop decision-making. The development of cybersecurity analysts, cybercrime procedures, or understanding of the phenomena within a group setting to achieve group consensus is not the purpose of this study, so the Delphi technique would not have been an appropriate design for this study.

Research Question

This study's overarching research question is as follows: What strategies do cybersecurity analysts of small businesses use to protect their systems from external cybersecurity threats?

Interview Questions

1. What methods do you use to protect your systems from external cybersecurity threats?
2. What are the challenges in obtaining C-level support for effective cybersecurity strategies within your organization?
3. What inefficiencies or lack of resources do you and your team experience utilizing industry-standard cybersecurity measures to prevent cybersecurity threats within your organization?
4. What industry-standard cybersecurity strategies effectively prevent inefficiencies as you protect the organization from cybersecurity threats?
5. What challenges do you and your team experience in utilizing industry-standard cybersecurity strategies to prevent cybersecurity?
6. What cybersecurity strategies do you and your team apply to prevent cybersecurity threats?
7. Which cybersecurity strategies are the most effective in reducing inefficiencies in preventing cybersecurity threats?
8. What other challenges or inefficiencies do you experience in adopting an industry-standard model to prevent cybersecurity threats?

9. What are the factors when selecting industry-standard cybersecurity strategies to prevent cybersecurity threats?
10. Which cybersecurity tools, techniques, or procedures provide the greatest protection within your organization?

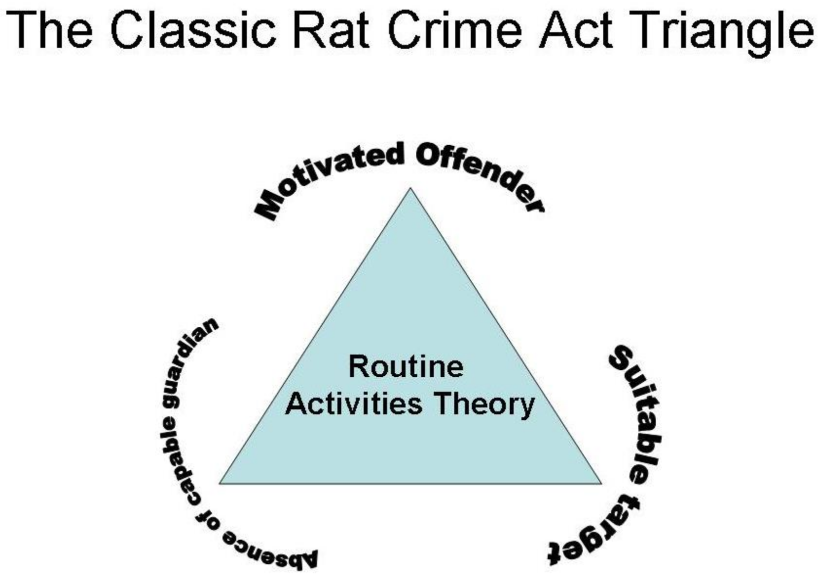
Conceptual Framework

The theory chosen for the conceptual framework is the routine activities theory (RAT). Cohen and Felson established the RAT in 1979 to explain crime as an event. Essential concepts within the framework RAT consist of the absence of a capable guardian, a motivated offender, and a suitable target (Kigerl, 2012). In 2012, RAT was applied to explore which demographic was the most prone to participate in cyberbullying (Jasinki & Navarro, 2012). Establishing and identifying crime as an event may provide information on possible cybercrime motivations concerning enhancing cybersecurity prevention capabilities.

Cohen and Felson's (1979) RAT was leveraged in this study to explore issues that provide the impetus for cybercrime activities referencing an offender, a suitable target, and the absence of a control or mitigation technique. Exploring participants' experiences of cybercrime as an event may provide insight into variables that propagate a lack of adequate application of cybersecurity strategies, which may also hinder the efficient usage of mitigation techniques to prevent cybersecurity threats in the small business domain.

Figure 1

Felson's Basic and Classic Routine Activities Triangle (RAT)


The Classic Rat Crime Act Triangle
Motivated Offender
Routine Activities Theory
Suitable target
Absence of capable guardian

Note. Felson's basic model for the concepts of RAT. Adapted from *On Opportunity and Crime*, by M. E. Sutton, 2012, Dysology (https://dysology.org/page8.html). Copyright 2003 by J. E. Eck and R. V. Clarke.

Definition of Terms

The following industry-related terms are provided to ensure that the reader has a clear and comprehensive understanding of the essential terms to be utilized in the study.

Capable guardian: A capable guardian has a "human element," which is usually a person who, by their mere presence, would deter potential offenders from perpetrating a crime that can exist by proxy, such as through closed-circuit television with someone always monitoring (Cohen & Felson, 1979).

Cybercrime: Cybercrime refers to criminal acts committed using electronic communications networks and information systems against explicit targets or targeted networks and systems (Lagazio et al., 2014).

Cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, and best practices, assurance, and technologies that can be used to protect the cyber environment, the organization, and user assets (Von Solms & Van Niekerk, 2013).

Cybersecurity strategy: A cybersecurity strategy is a plan for an effective, collaborative, enterprise-wide cybersecurity posture and defense (U.S. Department of Energy, 2018).

Data breach: A data breach is an incident that comprises unauthorized access to sensitive, protected, or confidential data, resulting in the compromise of the confidentiality, integrity, and availability of the data (Sen & Borle, 2015).

Incident response: Incident response is the action that encompasses all actions taken to restore normal IT service quickly and to minimize adverse impacts on business operations (U.S. Department of Homeland Security, 2015).

Information security threats: Information security threats are situations that may result in an information system compromise to harm business operations, business assets, and individuals, such as disclosure or unauthorized access of confidential information through social engineering and phishing (Ryan et al., 2012).

Intrusion detection system (IDS): An intrusion detection system is software or hardware designed to detect unwanted attempts at accessing, manipulating, or disabling computer systems, mainly through a network such as the internet (Bace & Mell, 2000).

Offender: A motivated individual with criminal intentions and the ability to act on inclinations (Cohen & Felson, 1979).

Personal identifiable information: Personally identifiable information (PII) is any piece of information used solely or in conjunction with other information to identify an individual by direct or indirect inference (U.S. Department of Homeland Security, 2012).

Social engineering: Social engineering is unauthorized access to restricted information or systems by deceiving individuals into revealing secure information (Posukhova & Zayats, 2014).

Suitable target: Individuals or property vulnerable or available (Cohen & Felson, 1979).

Assumptions, Limitations, and Delimitations

Assumptions

The assumptions, limitations, and delimitations provided for a study include discussing the study's inherent weaknesses. Analyzing common assumptions allows a real expectation of data that are as accurate as allowed, given the inherent assumptions as outlined. Assumptions are the information the researcher inherently accepts as accurate without actual confirmation of the evidence (Leedy & Ormrod, 2015). The assumptions noted for this study are as follows: I assumed that the organizations chosen would provide a good case for the concerns within small businesses today regarding preventing external cybersecurity threats. I assumed participants who were willing to participate in the study had sufficient experience meeting external cybersecurity threat prevention challenges within a small business. I assumed that the participants would provide data that would not be affected by the recent pandemic. The pandemic did not skew the budget, frequency of threats, staffing, and small business organizational resource allocations.

Limitations

Limitations are constraints in the study that the researcher cannot affect (Denscombe, 2013). The primary limitation of the study is my 36 years of experience in the field of IT, holding positions in management as a senior engineer, professor, and, more recently, a director of cybersecurity, which has the potential to influence the analysis of the data as well as my approach to the research and deriving themes from the data. Another limitation is gathering sensitive information that may not be transferred to other studies and may hinder the participants' ability to be forthcoming about the tips, tactics, and techniques utilized to provide a competitive edge and provide data. Additionally, some organizations may designate one position for threat management and another for threat prevention, which will dilute the data if organizations cannot gather the perspective from one position.

Delimitations

Delimitations consist of the researcher's choices that should be mentioned as they describe the boundaries set for the study to allow for the completion of the study (Denscombe, 2013). Data collection was confined to small business cybersecurity analysts in Texas rather than covering the entire southern region of the United States for accessibility purposes. Conversely, this study's focus analyzed external threats and forwent information regarding insider threats and internal threats. Additionally, there is a constraint on the initial sample size of nine small business cybersecurity analysts, considering the sensitivity of the data and the lack of resources in small business organizations. Another delimitation consisted of the participants being expected to have at least 1 year of experience in cybersecurity threat prevention and remediation.

Significance of the Study

Contribution to IT Practice

This study may provide strategies to cybersecurity analysts of small businesses who lack strategies to address external cybersecurity threats, thereby enabling small businesses to flourish. The Federal Bureau of Investigation (FBI) Internet Crime Report (2018b) reported that small businesses are the most attractive targets, with $2.71 billion in losses. This study may prove significant to IT practice as the analysis of small business cybersecurity strategies may provide access to practical models, controls, and mitigation techniques. Highlighting gaps in procedures and security awareness training of cybersecurity analysts in small businesses may protect personally identifiable customer data from cybersecurity threats. This study may contribute to IT practice by analyzing cybersecurity strategies utilized by cybersecurity analysts of small businesses to prevent cybersecurity threats. The findings from this study may provide a model to mitigate compromised personally identifiable customer information in small business organizations. Billions of confidential records and data are stored on networks and computer systems. In the first 6 months of 2019, 4.1 billion records and health-related data were compromised. Some of the most significant data breaches were perpetrated on AccuDoc Solutions and Equifax with third-party relationships with small businesses (Internet Crime Complaint Center, 2018a). Without the proper application and efficient utilization of cybersecurity strategies to protect personally identifiable customer information, society is vulnerable to the unauthorized access and illegal usage of personally identifiable customer data housed by small businesses (NIST, 2019b).

Implications for Social Change

The implications for positive social change include the potential for small business cybersecurity analysts to obtain the strategies and mitigation techniques that may prevent the exposure of personally identifiable customer information more adequately. These techniques may save small businesses valuable capital to reinvest in promoting local communities' job growth and funding to research the phenomena further.

A Review of the Professional and Academic Literature

The purpose of this pragmatic qualitative inquiry was to explore the strategies utilized by IT cybersecurity analysts of small businesses to prevent external cybersecurity threats. Critical analysis of the literature provided the impetus for my research in this pragmatic qualitative study and aided in analyzing strategies of nine small business cybersecurity analysts implemented in Texas to protect their systems from external cybersecurity threats efficiently. The primary focus of the study was to explore small business cybersecurity strategies to prevent external cybersecurity threats, analyze their effect on small business resources, and inform future cybersecurity prevention strategies and resource allocation. The research design development included nine small business cybersecurity analysts in various industries that may run the gamut of franchised, retail, or online entities. The number of participants is directly related to the topic's sensitivity for small business organizations and their reluctance to share open and honest dialogue about their security limitations within their organizations. Understanding these sensitive factors that are not often shared with third parties and conducting a research study within the onset of a pandemic (SARS-COV-2) may have adversely affected the recruiting of participants and the level of availability of cybersecurity analysts. Patience and ingenuity were needed to achieve data saturation in a timely and organized manner.

I focused on three essential concepts when reviewing the professional academic literature for this study: issues that center around the strategies utilized by small businesses to prevent cybersecurity threats, the applicability of RAT as a conceptual model to identify new strategies that are advantageous to small business cybersecurity efforts while utilizing a pragmatic qualitative inquiry research design to study the phenomena, as well as concerns that involve the offender, the target, and a capable guardian as referenced through the lens of RAT as a conceptual framework. In the context of this study, the offender is identified as the threat or hacker and their means, motive, and opportunity that present a viable threat to small businesses.

I addressed issues regarding the target, which in the context of this study, references small business cybersecurity and its strategies and the lack of a capable deterrent. I addressed the issue of a capable guardian in the context of this study, which is identified as cybersecurity analysts, controls, policies, procedures, resources, and strategies of small businesses. I executed a review of the academic literature using Google Scholar, the Walden Library, Science Direct, Ebsco Databases, Sage peer-reviewed journals, ACM Digital Library, ProQuest Central, Sage Direct, and IEEE Explore as chief sources for my academic research. I utilized the following search terms to initiate searches in these databases that reference RAT, social disorganization theory, crime opportunity theory, broken windows theory, situational crime prevention theory, small business cybersecurity, cyberthreats to small business, RAT, threat prevention, information security, small business risk, small business cybersecurity blueprint, small business threats, small business cybersecurity resources, small business cybersecurity resource allocation, small business cybersecurity strategies, incident response, small business cybersecurity regulations, small business cybersecurity innovation, small business cybersecurity policies, security and awareness, and SATE programs.

I also utilized the various referenced articles and search terms provided for each search as suggested links to other resources for correlating search terms to give an exhaustive review of the current literature. To provide a comprehensive review of the literature, I often utilized reference lists of peer-reviewed material as alternate sources of empirical subject matter to inform the basis of the study. My chief concern was to utilize contemporary publications, relying primarily on articles published in 2018 or later. In the spirit of providing a holistic point of view for the study, I also reviewed seminal articles and publications when researching the RAT conceptual framework and qualitative research design.

The content of the literature, as described in this review, references the history, current and contrasting views related to RAT, and its application to small business cybersecurity strategies. I selected seminal sources when applicable and obtainable. The chief focus of my literature review involves cybersecurity strategies of small businesses that include the methods utilized to achieve an environment where confidentiality, integrity, and availability are maintained. Small companies possess a finite number of resources that require strategies to effectively and consistently protect individuals' PII. The review of the literature will cover ethical, privacy, and human resource allocation concerns as they apply to organizational needs and how they affect the solvency of small businesses. Small businesses require strategies to provide a model for future resource allocation to maintain competent cybersecurity controls and cost-effective mitigation techniques.

I intentionally did not discuss internal threats to small business cybersecurity concerns such as insider threats and physical security threats. They do not directly relate to external cybersecurity threats and deserve the focus of a separate and more in-depth study for each phenomenon. I have gathered and reviewed more than 340 articles, peer-reviewed journals, and seminal resources while eliminating over 58 sources as irrelevant, repetitive, duplicative, and non-consequential in the context of my study. I was unable to review any material that specifically addressed the small business cybersecurity strategies and their analysis related to crime as an event that takes place with favorable conditions in the context of an offender, target, and a capable guardian as it relates to the context of my study.

To provide a holistic understanding of this literature review, I began with a discussion that reviews the conceptual framework and all its intricacies, as seen through the lens of securing assets for small businesses. Then I proceed to the relevant literature regarding the analysis of cybersecurity strategies to prevent cybersecurity threats. The review of cybersecurity strategies performed by small businesses starts with a definition of cybersecurity that discusses its importance to small businesses and what strategies are being applied. I then provide a discussion that analyzes those strategies, such as incident response and security awareness efforts, and how effective they are, given the limited resources utilized by small businesses, to achieve optimal security initiatives, as each organization outlines. I conclude the literature review by discussing innovative prevention techniques that evolved by studying relevant and contemporary cybersecurity strategies, given the finite number of resources that inherently plague small businesses.

The literature review consists of 146 articles relating to RAT and the inference of cybersecurity strategies that assist in the prevention of cybersecurity threats. In conducting the research, a set of standard resources utilized by small businesses' cybersecurity analysts was key in creating the context for the specific business problem. In addressing the particular business problem, a literature review consisted of incident response, security awareness, organizational buy-in, cybersecurity analysts, controls, policies, procedures, resources, and prevention strategies. I have proposed, through my rigorous study of the material, that effective strategies may be demonstrated that utilize time, the presence of a motivated offender, a suitable target, and whether the guardian is deemed capable, based on the conditions of each crime as an event as purported by Cohen and Felson (1979).

This pragmatic qualitative inquiry explored small businesses' cybersecurity strategies to prevent external cybersecurity threats and provided a holistic perspective on cybersecurity prevention strategies and their application. The proceeding section provides an exhaustive discussion of the conceptual framework and the current literature regarding cybersecurity strategies to prevent external cybersecurity threats for small business businesses.

Conceptual Framework

The conceptual framework for this study included RAT. In the following subsections, I provide an in-depth discussion of RAT and analyze both supporting and contrasting theories.

Evolution of RAT

RAT is a subfield of crime opportunity theory that focuses on situational crimes. Marcus Felson and Laurence E. Cohen first proposed an explanation of this theory in 1974 to explain the crime rate changes in the United States between 1947 in 1974 (Cohen & Felson, 1979). It should also be noted that generations of victimologists have integrated lifestyle exposure theory and RAT into what they now call lifestyle-routine activities theory (LRAT) of criminal victimization, highlighting the importance of an individual's lifestyle and routine activities in generating opportunities for victimization (Messner et al., 2007). The utilization of RAT was a methodology applied in the analysis of an investigation focusing on online criminal behaviors that referenced participant experiences of crime as an event that provided information on possible cybercrime motivations translating into attacks on their systems. (Pyrooz et al., 2015). The theory has been widely used and applied in the past 30 years as it has become one of the most cited theories in victimology (McNeeley, 2015). However, unlike criminological theories, routine activity theory applies the perspective of crime as an event that closely relates the crime to the environment and emphasizes its ecological processes, thereby shifting academic attention away from average offenders and focusing more on the environment and a specific set of circumstances that must exist for the crime to take place (Cohen & Felson, 1979).

While applying the concepts of RAT, three necessary conditions must apply: the presence of a motivated offender, the presence of a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). All these conditions must come together in time and space for the crime to be committed. The lack of any of the three elements is sufficient for the crime to be prevented. A connection must be made between the motivated offender and the suitable target. The connection of the motivated offender and the suitable target would be the equivalent of the hacker and the small business, respectively, which would be deemed as required elements adding varying levels of time, space, and environmental factors to the crime event.

RAT has its foundation in human ecology and rational choice theory, as Cohen and Felson (1979) described. Routine activity theory has been heavily utilized to study sexual crimes, residential burglary, robberies, cybercrimes, and corresponding victimizations. As Hindelang et al. (1978) described, RAT often regarded the lifestyle theory of criminology as similar. Routine activity theory has been utilized frequently in multilevel frameworks and social disorganization theory in understanding various neighborhood crimes.

Routine activities mediate the similarities connecting demographic characteristics and victimization (Bunch et al., 2015). The analytical focus of routine activity theory approaches studies from a holistic viewpoint. It derives data from a broad-scale shift in victim and offender behavior patterns as it focuses on detailed crime events and offender behavior. RAT assumes that an offender with the means, motive, and opportunity can successfully commit a crime when the conditions are favorable, as posited by Cohen and Felson (1979). The theory assumes that the victim plays an intricate role in choosing to be victims by not placing themselves in a position where crime can be committed against them. This theory provides an interesting perspective on the varying factors of victimization and prevention strategies that may well translate to cybercrime.

Cohen and Felson (1979) decided to present RAT to aid in disseminating human ecology theory, as posited by Hawley in 1944. Hawley's research demonstrated the belief that three elements withstanding define how our lives are connected that consist of timing, tempo, and rhythm (Cohen & Felson, 1979). These conditions coincide with what Hawley believed to be factored into how these elements influence the frequency of crime rates. When these factors are applied to cybercrimes and the ability of a motivated offender to execute a successful breach against a target that lacks a capable defender, we can identify strategies that may prove to be advantageous for small business organizations (Messner et al., 2007). These strategies would involve manipulating environmental factors and how this would affect the probability of mitigating vulnerabilities.

When applying theories associated with RAT, there are spatial elements to a physical crime event and correlating conditions that must exist for the crime to be executed, as posited by Cohen and Felson (1979), consisting of a motivated offender, suitable target, and lack of a capable guardian. It is not readily apparent that research exists to utilize the factors from a physical crime that can be correlated scientifically to curb crime patterns based on data analysis realized in cybercrime. Reyns et al. (2011) argued that a networked system could be the space for the interaction consisting of the target and the offender as a substitute for the physical environment. Closing the gap between cybercrime and physical crime may provide cybersecurity analysts with the data policymakers require to enact laws needed to curb cybercrime. Wen-qun (2006) also asserted that the divide exists between technologies used to execute cybercrime and real-world physical crimes, which lends itself to difficulty in adequately mitigating cybercrime. Griffioen et al. (2021) proposed that the connection is made between the divide between cybercrime and physical crime, as well as innovative internal applications that can be framed based on these factors leading to positive change that efficiently mitigates cybercrime by adding greater obscurity to a system hindering the external attacker's ability to gain knowledge within a network. In this vein, reviewing cybercrimes through the lens of RAT offers a unique perspective on mitigating cybercrimes in small business organizations. When applying soft measures, in reference to an external threat and their utilization of anonymity, such as geospatial techniques and time-varying dynamic models, Khey and Sainato (2013) proffered that the correlates and spatial distribution of organizational data breaches in the United States were advantageous in providing data reports of high domestic cybercrime in key areas. Geospatial techniques, MTD, and time-varying dynamic models may aid in threat mitigation when translated to cybercrime, improving the efficacy of encryption services and providing data that can advance a higher level of administrative policies to reduce cybercrime. Henson et al. (2016) noted that physical interaction within a specific time frame might not be a mitigating factor when leveraging RAT in cyberspaces if the target and the offender eventually converge. These techniques may lead to directing reinforcements needed as the efficacy of the model was proven to decrease the number of compromised hosts, including after a data breach, as posited by Xiong et al. (2019). The study's researchers called for integrating spatial analysis and tactical decisions to reduce domestic cybercrime. These techniques enhanced threat prevention across geographic locations and organizations as this model may prove to be applicable across segments of cybersecurity as well.

Considering the spatial elements as it applies to RAT, which consists of time, space, and the motivated offender's perception of an ideal target, it is vital to understand how to reduce the risk of victimization. By applying RAT principles, IT cybersecurity analysts may have adequate leverage in contributing to reducing the risks associated with victimization-related events (Choi et al., 2016). When reviewing the research, the researcher's goal was to provide data that would measure the effectiveness of a more capable guardian while reducing the suitability of the targets to prevent, intervene, and respond to incidents (Choi et al., 2018). When viewing the IT problem through the lens of RAT, it would prove logical to understand the areas we can better affect positive change through the creation of compensating controls, which would be the element of the capable guardian and the suitable target being the IT cybersecurity analyst and the small business respectively (Messner et al., 2007). The motivated offender's perception of the target and the conditions regarding the suitability of the target will be in direct response to the controls implemented to enhance guardianship, presumably leading to affecting their motivations.

Researchers have indicated that RAT is a theory established to apply across multiple criminal activities (Leukfeldt & Yar, 2016). To what extent can theoretical concepts based on the cyber world effectively be applied to a virtual environment? Theoretical, as well as the analysis of empirical studies, have provided a myriad of mixed results. Analysis of several studies has shown that some of the elements of RAT, when applied to cybercrime, are more applicable than others. Kulig et al. (2019) posited that the original concept of RAT did not provide an adequate definition of the attributes of a motivated offender, as Cohen and Felson conceded this limitation and indicated future research was needed to understand offenders' motivation for the crime. Visibility was noted as being an apparent factor in cybercrime victimization. Accessibility, as well as personally capable guardianship, have shown mixed results. Cohen and Felson (1979) argued that capable guardianship was an essential factor in the" crime triangle" concept.

When applying the theoretical framework of RAT while referencing the data to provide a better understanding of how to mitigate cybercrime through effective change, it would be deemed prudent to rely on data regarding the visibility of cyber victimization and the effect of the conditions on the motivated offender and how to create an atmosphere to curb that motivation (Choi et al., 2016). The need to supply a capable guardian with tools to effectively execute their primary function in the crime triangle, as well as how to manifest conditions to achieve an even higher level of capability, the suitability of the target, and how to propose actions to create a less suitable target, may prove to add a layered prevention strategy whether those actions pertain to the environmental, spatial, or absence of any of the three required elements for a crime to be committed (Choi et al., 2018).

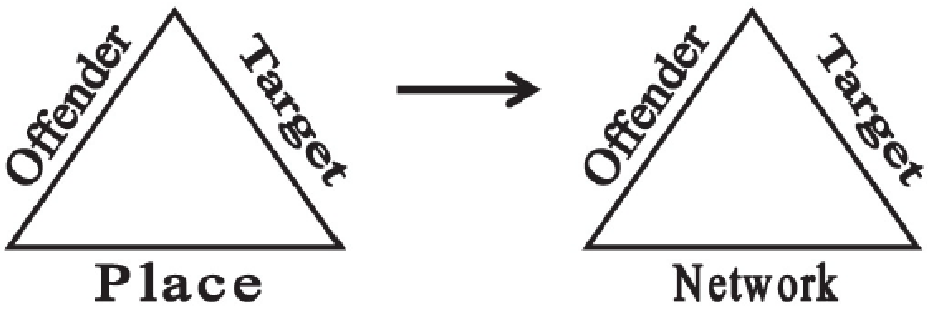
One of the understood factors of criminology is the theory that crime will consist of three factors: motivation, opportunity, and the lack of a capable guardian. These factors can apply in an individual incident as well as established trends. Derived originally to explain physical crimes, it is equally applicable across cyberspace (Grabosky, 2001).

LRAT has been modified over time to fit situational crimes beyond the parameters for which it was intended. Some theory applications were applied to crimes across long distances, such as postal crimes and telemarketing fraud (Eck & Clarke, 2003; Reyns et al., 2011). Eck and Clarke (2003) argued that even though the theory was intended to apply to crimes where the offender was in direct contact with the target, it should equally apply to crimes that provided some distance between the two. In instances of RAT, which was initially viewed to apply to crimes of opportunities, usually resulted in the conditions that require the intersection of time and space of the essential elements for the crime to take place, consisting of a motivated offender, a suitable target, and the lack of a capable guardian as posited by Mohammad and Nooraini (2021). However, many crimes do not readily meet or involve time and physical space.

Crimes that consisted of a considerable distance were referred to as “systems problems,” arguing that the elements of the crime may interact at some distance, as cited by Eck and Clarke (2003). This added dimension would appear to be in direct opposition to RAT. Vakhitova et al. (2019) noted this change by referencing the crime triangle from a systems perspective. The adaptive crime triangle and the rationale for its utilization are reasonably logical and applicable to RAT. When motivated offenders and suitable targets exist within the same network, the network can be substituted for the physical location necessary for any physical crime within proximity Reyns et al. (2011).

Figure 2

Adaptations of the Crime Triangle



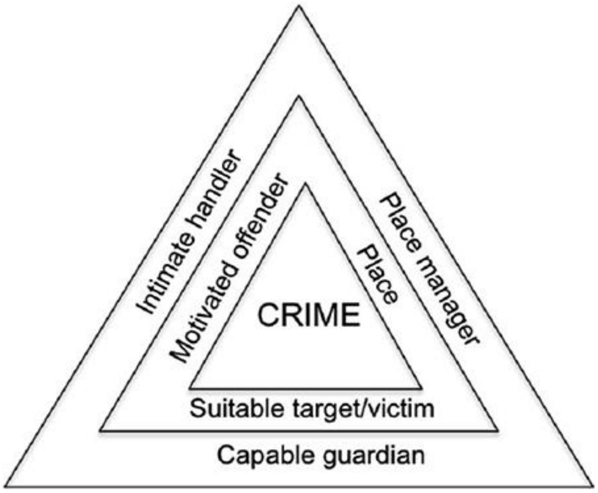
Note. A comparison of network vs. physical crime. Adapted from "Classifying Common Police Problems: A Routine Activity Approach," by J. E. Eck and R. V. Clarke, 2003, *Crime Prevention Studies*, *16*(1), p. 13 (https://www.researchgate.net/profile/John-Eck/publication/258440181_Classifying_Common_Police_Problems_A_Routine_Activity_Theory_Approach). Copyright 2003 by J. E. Eck and R. V. Clarke.

Reyns et al. (2011) posited that the application of the network-based crime triangle displays how RAT can be expanded to include crimes that take place with distance as a factor in which motivated offenders and suitable targets do not intersect at a physical location. In the act of cybercrime, as the motivated offender and the suitable target exist within the same network, the distance between these elements is not as exaggerated as one would think. Studies, where researchers have specifically utilized the systems approach, have indicated that the concept of RAT can be successfully extended to cyber-related crimes (Reyns & Henson, 2015).

Elements of cybercrime are in direct contact via a virtual environment, even though they may reside on different sides of the globe. The virtual environment links time and space between the motivated offender and the suitable target. The capable guardian would still play a significant role in this intersection of time and space; as the guardian's capability is increased or decreased, it may affect the offender's motivations.

Figure 3

The Crime Triangle



Note. Adaptations of a crime triangle. Adapted from *Oxford Research Encyclopedia*, by R. V. Clarke and J. E. Eck, 2003, *Criminology and Criminal Justice* (https://oxfordre.com/criminology). Copyright 2003 by Oxford Research Encyclopedia.

The crime triangle has been updated to include a more detailed analysis of the intersection of the elements affecting crime and criminal behavior with external factors (Vakhitova et al., 2019). The motivated offender class is measured by the zeal they are willing to offend despite the negative consequences, often weighing a cost versus the reward factor. The motivations can be as simple as gaining a profit or a matter that may involve an instance where the convergence of time, space, and opportunity was suitable for committing the crime (Kulig et al., 2019). There are several mitigating factors as the motivated offender chooses a target. These factors consist of ease of access to the target, the ability to carry out the crime without being detected, the portability of the target, and the ease it can alleviate (Elmaghraby & Losavio, 2014).

The capable guardian provides a constant presence consisting of individuals whose very presence deters criminality, provides an avenue for a speedy recovery, or sanctions against the offender that can be applied in cyberspace as posited by Hawdon et al. (2017). As capable guardians successfully oversee suitable targets, motivated offenders are surveilled by handlers, and managers monitor compliant locations, crime prevention can be achieved (Choi & Lee, 2017). When serving as a theoretical lens, RAT may be leveraged to provide an observation that increases the capability of guardianship and decreases the target suitability of small businesses while varying the factors of the capable guardian’s presence as a strategy to mitigate the risk of cybersecurity threats.

Analysis of Supporting Theories

General Systems Theory (GST). Von Bertalanffy (1969) developed GST intending to focus on the complexity and interdependencies of systems. At its core, the fundamentals of GST reside in the system wholeness, collaborative interactions and continued relationships within a system, and the analysis of systems that provide pathways to understanding and probing the intricate characteristics of the interconnected whole of a system (Von Bertalanffy, 1969). Researchers utilize GST through a theoretical lens to probe the totality of an organizational system by gathering data from related functions that include ownership and guidance. General systems theory comprises several elements to understand the wholeness of a system that provides emergence, evolutions of adaptation, self-organization, dynamics in systems, complexity science, and science of network (Sturmberg et al., 2014). Conceptually, GST is similar to RAT as the theories require observation of physical conditions that center around the analysis of systems; however, GST is focused on the totality of the entire system that is complex, with various components working together to complete a task while RAT is focused on the convergence of three elements in time and space to achieve the desired outcome as posited by Mohammad and Nooraini (2021). While GST provides a lens for analyzing the totality of an open system with various components, RAT is a more appropriate lens to apply to this study because of the focus on the three converging elements and a more centered approach for each of those elements.

Rational Choice Theory (RCT). The RCT was introduced in 1986 by Cornish and Clarke to provide an additional theory to assist in thinking of the varying levels of crime control that center on the offender's motivations, leading to the reasoning of their choices (Cornish & Clarke, 1986). The theory is applied through a lens that assumes that offenders make several calculations before committing an offense that would benefit the offender. These calculations are weighed heavily before the crime occurs (Cornish & Clarke, 1987). Succinctly, the attacker selects their targets to fulfill a financial or social need (Cornish & Clarke, 2008). Three defining elements of RCT consist of an agent, choice, and opportunity to act (Cameron & Kornhauser, 2015). When looking through the lens of RCT, criminal decision-making is made up of various factors other than recognizing good opportunities, and even when the choice is sudden, there is some forethought (Cornish & Clarke, 2008). Theoretically, there are some similarities between

RAT and RCT. However, RCT focuses on the offender and their calculated motivations and benefits.

In contrast, RAT focuses on three elements: the motivated offender, suitable target, and capable guardian that intersect within time and space. Cornish and Clarke (2008) expanded upon the concepts regarding RCT formulation by introducing yet another dimension which they defined as the constellation of perceived opportunities, costs, and rewards relating to specific types of crimes. While RCT shows promising concepts that could apply to the study, the focus is primarily on the offender and the varying levels that affect motivations. Hawdon et al. (2017) posited a more compelling comparison as RAT was a concept applied across cyberspace. Viewing the study through the lens of RAT provides a broader look into each of the three elements that intersect within time and space, allowing for a richer analysis of the theory to affect change more effectively.

Analysis of Contrasting Theories

Lifestyle/Routine Activity Theory (L-RAT). Cohen et al. (1981) explored the consolidation of lifestyle-exposure theory with routine activity theory. This new consolidated model was initially referred to as “the opportunity model of predatory victimization” (p. 507). This amalgamation of theories centered around five concepts including guardianship, exposure, target, distance, and location compared to potential offenders, attractiveness, and definitional properties. Definitional properties reference the opportunities or constraints presented based on a set of conditions perceived by the potential offender as risk worthy or non-advantageous in the commission of a particular crime. Lifestyle-exposure theory and RAT were combined, sharing theoretical lenses to explore victimization at an individual level (Messner et al., 2007). Routine activity theory and L-RAT frameworks are, in many cases, merged to meet various applications to gather a specific set of data points; however, this has led to the framework being changed into many forms confusing the individual components for each application of the theory (Hindelang et al., 1978). The conversations surrounding the studies regarding relationships between L-RAT concepts and victimization display that many forms of victimization are more likely to occur at home; however, this data is at direct odds with Cohen and Felson’s (1979) study examining household activity ratios and crime rates. In comparison, L-RAT may be frequently utilized interchangeably with RAT, with notable differences surrounding key concepts that may cause conflict and confusion, creating results that may be indiscernible. The RAT theoretical lens focuses on the convergence of a motivated offender, a suitable target, and the lack of a capable guardian sharing space and time as L-RAT provides a focus for the risk of victimization through lifestyle choices that increases due to increasing probabilities (Choi et al., 2018). L-RAT may be an appropriate lens to view the probability of a crime taking place based on exposure on an individual level; however, RAT is a more appropriate lens for viewing strategies to prevent external cybersecurity threats.

Lifestyle Exposure Theory (LET). Lifestyle exposure theory emerged in 1978 as a comprehensive model designed to explain variations in the risk of victimization (Hindelang et al., 1978). Hindelang et al. (1978) posited that those individuals are more likely to become victims of crime simply due to their lifestyle variations. Hindelang et al.

(1978) defined lifestyles as “routine daily activities, both vocational activities (work, school, keeping house, etc.) and leisure activities” (p. 241) and argue that individuals whose activities enter the path of potential offenders are more likely to become victims due to proximity to offenders, their lifestyles, and repetitive activities. This theory would conflict with L-RAT by repetitive nature, and rational thought individuals would cease such behavior if rational decisions were made after analyzing the risk regarding victimization. Reyns and Henson (2015) posited that LET exposes an individual to victimization risk due to personal qualities of lifestyle. Looking through the lens of LET provides an atmosphere heavily determined by probabilities regarding an individual’s lifestyle choices. The individuals are at risk of victimization due to the concept that involves the type of lives they lead, such as continually frequenting high-risk areas during high-risk hours of the day or night (Hindelang et al., 1978).

The theory proposes that “routine activities may predispose some persons and their property to greater risks, but the selection of a particular crime victim, within a socio-spatial context, is determined by the expected utility of one target over another” (Miethe & Meier, 1990, p. 245). Also, it identifies proximity to motivated offenders, exposure to risky situations, target attractiveness, and the absence of capable guardians as the key factors that determine the likelihood of criminal victimization. Conceptually, LET may have some similar concepts that may apply in this study, such as target attractiveness and proximity to motivated offenders; however, the determinate factors and concepts that surround victimization issues, regarding little to no focus on the capability of the guardian, as well as criminal motivational theories are not very well defined within the model as posited by Vakhitova et al. (2019). These factors would prove that measuring them would be difficult and even harder to validate in the physical environment for which they are designed, which would be exacerbated in the cyberworld; therefore, RAT would be the most appropriate theoretical framework for this study.

Cybersecurity Strategies

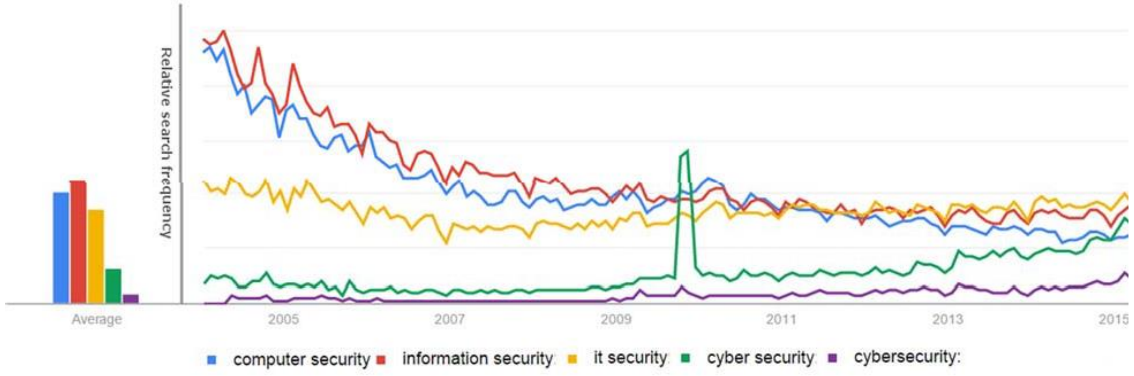
Defining Cybersecurity

The terminology used in defining cybersecurity has changed significantly over recent history. As Von Solms and Von Solms (2018) articulated, the meaning of the term cybersecurity translates to protecting data from unauthorized access or attacks fitted for exploitation. The Association of Computing Machinery Joint Task Force (ACMJTF) on Cybersecurity Education (2016) utilized a broader, more comprehensive definition encompassing technology, people, information, and processes to enable assured operations and creation and operation analysis testing secure computer systems. The terminology frequently used to describe the phenomena was “Computer Security,” “IT Security,” or “Information Security” (Schatz et al., 2017). While those within the profession understood these terms, each term carried a specific meaning as the implications were general enough to be understood by the broader population from other disciplines (Schatz et al., 2017).

It would behoove the cybersecurity community to have a unifying vocabulary to identify and suppress cybersecurity threats concisely and effectively. The lack of a consistent definition as well as the spelling of “cybersecurity” was in question as some organizations and some countries utilize a two-word spelling (cyber security) rather than the popular one-word spelling more heavily utilized in the US (Congressional Research Service, 2014). In the future, I will utilize a one-word spelling for uniformity and relevance. The term “cybersecurity” was utilized pre-2009; however, the terminology gained considerable popularity after U.S. President Barack Obama 2009 proclaimed, “I call upon the people of the United States to recognize the importance of cyber security and to observe this month with appropriate activities, events, and training to enhance our national security and resilience” (The White House, 2009). The overwhelming impact of the proclamation, in the form of a press release, can be illustrated through the utilization of a chart that highlights a conspicuous increase in a Google search trend for the term” cyber security” concerning the total number of searches executed between 2004 to 2015 in comparison to “information security” and “computer security.”

Figure 4

Google Search Trends for Security 2004–2015



Note. Trends for the search term cyber security vs. cybersecurity. Adapted from ‘Towards a More Representative Definition of Cyber Security,” by D. Schatz, R.

Bashroush, and J. Wall, 2017, *Journal of Digital Forensics Security and Law, 12*(2), p. 54 (https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl). Copyright 2017 by ADFSL.

As cybersecurity has been defined in many forums, few distinguish between cybersecurity and information security concepts. When discussing cybersecurity, in most of the literature, the term is utilized as an all-inclusive term as definitions vary (Schatz et al., 2017). Cybersecurity encompasses the protection of data and assets, some of which are not stored or communicated, going beyond the traditional views of protecting technology but also covering the individual to the Internet of Things (IoT) to societal interest that includes critical national infrastructure as well as anything or anyone that can be connected via cyberspace (Kremling & Parker, 2017). The Association of Computing Machinery Joint Task Force (ACMJTF) on Cybersecurity Education (2016) additionally posited that it is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries (p. 1). Buch et al. (2017) proposed that the term cybersecurity is utilized to refer to an internet-based form of security to protect your stored online information.

Von Solms and Van Niekerk (2013) proposed the following definition of cybersecurity:" Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, the organization, and user assets." Since I focused the direction of this study to include the analysis of small business cybersecurity strategies to prevent external cybersecurity threats concerning RAT rather than security concepts, guidelines, and risk management approaches of cybersecurity, as well as the holistic view of securing information systems online, I have utilized Von Solms and Van Niekerk (2013) descriptive definition for this study.

Challenges of Small Business Cybersecurity

Cybersecurity has become essential in the everyday lives of individuals, businesses, governments, and countries worldwide. As individuals become more efficient and improve the human condition, they inherently increase their digital footprint while creating new information delivery and storage (Doneda & Almeida, 2015). Cybercriminals have been paying attention to the progression of tools, tactics, and techniques to compromise these systems (Ene, 2019). Hagen and Albrechtsen (2009) pointed out that obtaining competencies in guaranteeing cybersecurity resides in adequately predicting, monitoring, and effectively addressing cybersecurity challenges. As people and organizations become increasingly attached to the digital world, protecting their data and securing their connections to the IoT is paramount.

New strategies and concepts need to be formed for this new era to obtain efficient and effective cybersecurity for many organizations with cybersecurity shortfalls. Radziwill and Benton (2017) asserted that budget was a perpetual concern amongst small businesses that seek to implement efficient cybersecurity methods and protocols. According to West (2017), the loss of revenue attributed to data breaches is calculated to be in the millions, and the incalculable loss of privacy for those individuals who have been victims of data compromise. This shortfall would put organizations in a position to make crucial decisions about protecting their PII from cybersecurity threats in smaller organizations. Adding to the dilemma of creating secure and rational cybersecurity decisions, a small business may forgo external testing, including vulnerability scans and penetration testing exercises (Kabanda et al., 2018).

When approaching small businesses, the managed services provider (MSP) is in direct contact with the CEO due to the company's inability to hire a security specialist due to budgetary constraints and a lack of resources (Kabanda et al., 2018). In some organizations, cybersecurity is foreseen as creating a lack of upfront revenue and is looked upon as a cost center rather than a valued resource within a company; however, care and due diligence must be exerted as these small businesses are entrusted with private, sensitive, and financial data which they store and process resulting in a small cost in comparison to the consequences that can result in loss of life via the compromise of critical infrastructures (Mangelsdorf, 2017). The data that these companies hold must be protected. Therefore, without a cybersecurity plan or policy in place, it may lead to the organization's inoperability after one security breach due to fines, reputational degradation, and punitive damages. Munteanu (2017) posited that the main caveat that should be addressed is that cybersecurity analysts should be aware of their policies' limitations and plans to reduce cybersecurity threats effectively.

Cybersecurity provides countless advantages, and it is ubiquitous in society and business. Organizational managers largely struggle to address the issue of cybersecurity (Philip & Salimath, 2018). Ayereby (2018) pointed out that managers often have issues with understanding the complexities of associated risks that deal with human errors, environmental concerns, as well as intended cyberattacks that can cause strategic business or mission failures. In the context of the implementation of cybersecurity, as it relates to small businesses, the theme is often restated that small businesses lack the strategies and resources to prevent external cybersecurity threats effectively. The finite resources of the organizations do not allow for much innovation or qualified personnel to provide “outside of the box” analysis of cybersecurity incidents (Almeida et al., 2018). Small businesses must make very cost-effective decisions when applying budgetary and cost constraints as they do not have the privileges of the larger, more successful businesses as this plays a role in the quality and amount of staffing, training, and technology when implementing their cybersecurity strategy (Kobe & Schwinn, 2018).

When navigating a small business, there are several concerns when outlining a cybersecurity strategy and addressing policy initiatives. There are three main areas of concern when applying a finite set of resources: staffing, financial, and resource deficits (Selznick & LaMacchia, 2018). Small businesses must strike a delicate balance between integrating new internet-based technologies to remain competitive and formulating a cybersecurity strategy that can effectively secure and maintain those systems (Berry & Berry, 2018). Cybersecurity threats can cause significant losses within a small business. The Ponemon Institute (2019) reported that small businesses are at greater economic risk per employee than larger corporations of 500 or more as their losses were comparable in dollars lost per employee, thus creating a more significant financial impact due to their smaller size, a lesser amount of capital, and finite resources. After analyzing the data, losses are potentially created from a lack of proper cybersecurity strategies linked to a lack of resources to mitigate those threats. It is a vicious cycle that must be addressed appropriately to remain viable.

The effect of lacking properly managed resources for a cybersecurity strategy can directly affect the business's finances, reputation, and objectives (Cunningham & Head, 2019). As a result, a lack of resources may lead to end-users participating in risky internet behavior. The average user has no concept of cybersecurity processes that protect systems from compromise, including security and awareness, one-time password generators, Secure Sockets Layer, and two-factor authentication (Berry & Berry, 2018). Researchers have found that the ability to account for the human factor in data breaches provided by security controls fails to address this factor. Small businesses lack adequate resources to adequately provide robust security controls and comprehensive cybersecurity training programs (Ricci et al., 2019).

Cybersecurity is needed in every realm of society, and adequate cybersecurity strategies that protect the data of every individual and their ability to participate in commerce safely are a mainstay and necessary for businesses to protect customer data. Burley (2017) professed attackers focus on people rather than technologies, as organizations focus a large part of their cybersecurity budget on technical and monitoring capabilities. Additionally, Tyler (2018) agreed that only one employee is needed to bypass the most secure technological controls causing severe damage to the organization. When these systems become more intertwined, it adds sophistication and complexity. It will inherently add another layer of risk that can damage consumer confidence in an organization if not adequately mitigated (NIST, 2018). Small businesses are advised to implement strategies that NIST has created, more succinctly frameworks found in the NIST SP 800 series, formulated in response to the humbling statistics surrounding data compromise that was becoming a sensitive and urgent issue due to its growing prevalence (Almutairi & Riddle, 2018). As small businesses adopt this publicly available framework entitled NIST SP 800-61 Rev. 2, many concerns cannot be addressed that affect how small businesses protect their infrastructure from cybersecurity threats (Raghavan et al., 2017). NIST SP 800-61 Rev. 2 can be utilized to effectively provide an outline to identify its most valued assets and provide a strategy to protect its infrastructure; conversely, small businesses may possess many concerns that cannot be addressed by strategic models and processes alone.

Small businesses must make critical decisions that affect their bottom lines, such as hiring qualified cybersecurity analysts, purchasing threat detection and threat prevention security systems, and adequately maintaining operational duties such as training and crucial updates for each system and staff with an expectation of mitigating their cybercrime losses while decreasing cost by exploring new technologies (Stergiou et al., 2018). Ayereby (2018) also noted that senior management should understand their decisions on information systems and their long-term effects. Cook (2017) posited that new and groundbreaking approaches, ideas, and cost-effective strategies are warranted. Following an industry framework will not provide a comprehensive approach to the various security vulnerabilities that are diverse and suspectable to human errancy. The balance weighed for small businesses is indelibly tied to the amount of risk an organization is willing to accept. According to Sechel (2017), most organizations depend upon a risk calculation that provides a formula that cannot adequately assess or identify risks. Stewart (2018) further argued that one of the single most salient points within the current risk management models being proposed by several institutes is using very sophisticated formulas and mathematics. The threat analysis is centered around the cost of implementing a security control or mitigation while providing a prediction, based on data, that the likelihood of a threat materializing and outweighing the cost of perceived security control or mitigation will be avoided (ISC, 2020). In an analysis of these concepts, potentially, they require that the data and risk management models are fairly accurate. The revelation of significant data breaches in the media has shown this hasn't fared well for small businesses in recent history.

Cybersecurity's Role in a Small Business

Small businesses are continually a popular target of the hacker community as noted by Almeida et al. (2018). Small businesses lack the adequate resources to enable their cybersecurity strategy to adequately meet the barrage of cybersecurity threats as new exploits are being created in cyberspace daily. Harris and Patten (2014) indicated that larger businesses and corporations are empowered with adequate resources to recruit, train, and implement diverse and experienced cybersecurity analysts and provide the latest technologies in threat detection, threat prevention, and incident response. These strategies would seem to be industry standards for comprehensive threat mitigation and incident response methodologies; however, small businesses often find it a difficult balance between cultivating revenue streams that involve the processing and storing of PII, investing in digital technologies to grow their business to remain competitive, as well as providing adequate cybersecurity strategies to ward off cybersecurity threats (Selznick & LaMacchia, 2018) effectively and efficiently.

Cybersecurity resource allocation in small businesses is a delicate balance between the C-level executives, of which their buy-in is a significant factor in approving cybersecurity initiatives, and its perception as some view its function as a cost rather than a needed investment that protects their organization from company ending data breaches and liabilities (Raghavan et al., 2017). In many cases, the issue of cybersecurity can be distilled into notions that cybersecurity is just a drafted template of a policy that satisfies customer fears rather than a holistic approach that provides adequate protection from data compromise that includes endpoint protection, threat detection, threat prevention, incident response, as well as security and awareness training (Selznick & LaMacchia, 2018). Systems that consist of endpoint protection, threat detection, threat prevention, incident response, and training required for effective, efficient mitigation and eradication of threats are expensive and play a significant role in how small businesses approach cybersecurity hygiene (Raghavan et al., 2017).

The protection of a consumer's private data is paramount to the success of a small business as customers would fail to patronize an institution that does not regard their personal private information as such, leading to lost revenue and consumer confidence in the business (Gwebu et al., 2018). Vendor associations also expect a heightened level of cybersecurity practices through all phases of the supply chain. Often, threats originate from partner corporations that do not share or provide the same level of cybersecurity compliance as their counterpart (Raghavan et al., 2017).

Sound cybersecurity policies that include contingency planning protect not only the small business but also include protection for any vendor associations, as well as vulnerability rating systems that determine whether commerce can be conducted safely with the small businesses, as well as protect the confidentiality, availability, and integrity of the consumer and the associated vendor providing a road map to be followed for current and future sales initiatives and vendor associations (Raghavan et al., 2017). The role of cybersecurity, C-level buy-in, management, and its implementation within a small business must be shared by all, from the unheralded cybersecurity analyst to the Chief Information Security Officer of the organization (Rothrock et al., 2018). For example, the entire organization may be considered incident response. All employees may be encouraged to work together to create new initiatives conducive to researching the most effective, efficient, and cost-effective strategies that allow the strategies to permeate throughout the organization.

Small Business Breach Susceptibility

In the United States, in 2018, 70% of all data breaches targeted small businesses as they typically lacked the cybersecurity resources of larger businesses (Small Business Administration, 2018). Small businesses are very susceptible to an attack. These attacks leverage numerous vulnerabilities in scale, but more often, these attacks likely will go unreported as small business data breaches don’t receive the attention garnered by larger counterparts (Iverson & Terry, 2018). Data breaches have become so widespread that it is now seen as a part of the process of engaging in commerce, as threats are ever-changing and evolving (U.S. Department of Commerce, 2017).

Data can be used to expose faults as vulnerabilities to be exploited in a network and are classified as a security threat to an organization (Kaukola et al., 2017). With numerous vectors and exploits that can be manipulated to enter a network, small businesses find themselves at a disadvantage, in comparison to larger firms, due to a lack of resources and the frequency of advanced persistent threats (APT) that do not allow for the most advanced technologies and training to identify and remediate such advanced persistent threats (Liang et al., 2018). The balance for smaller firms is to manage growth, technology, and innovation while understanding the escalating risks, implementing state-of-the-art security technologies, and assessing the threat landscape (Martin et al., 2017).

Due to the finite resources, small businesses cannot appropriately hire experienced cybersecurity analysts that can adequately identify and remediate advanced persistent threats (APTs). According to Prajogo et al. (2018), once small business leaders begin to understand cybersecurity holistically as one system and understand how every component interacts with one another, small businesses will be better positioned to combine resources, increasing the chances of preventing cybersecurity threats. The unsuspecting user who is not well-versed in incident response or security and awareness is like any other untrained user within an organization. The unsuspecting user remains one of the weakest links in the cybersecurity network, as posited by Budzak (2016).

Larger corporations have the resources to institute Security Awareness Training and Education (SATE) programs that can change behaviors and correct any reoccurrences of unwanted behavior. The correction of unwanted behavior is achieved through a rigorous system of testing that alerts an organization when an employee clicks on an email from a suspected external threat and has utilized social engineering techniques to enter the network (Prajogo et al., 2018). The SATE program provides data on each user that can be modified to fit each user's behavioral pattern. Over time, the program allows the user to effectively identify threats from external sources, thereby decreasing human risk to the organization (Jackson, 2018). The methodologies presented are a few strategies that small businesses may be unwilling to pursue due to a lack of resources and proper threat intelligence. Without the right techniques to identify where the allocation of resources will best meet the organization's goals for the near future, it will ultimately leave vulnerabilities unmitigated and the acceptance of a high-risk tolerance as a cybersecurity strategy.

Small Business Cybersecurity Hygiene

For a small business to meet compliance, cybersecurity analysts must relay concerns and cybersecurity needs while remaining consistent in utilizing systems that ensure its infrastructure's confidentiality, integrity, and availability (Kakucha & Buya, 2018). Smaller firms must identify cybersecurity practices that effectively relay real threats to the organization and stay ahead of the curve. Every improperly managed resource can cost the organization valuable time and resources, resulting in missed opportunities to acquire competent staff and overall competitiveness. These factors play a role in acquiring technologies to help mitigate specific risks to the organization (Markey, 2018). Small businesses provide very little innovation when implementing controls, as their controls often mimic those of the typical end-user. A small business is tasked with overcoming many obstacles when trying to maintain viability and create a culture that promotes safe cybersecurity practices, as the employees must possess the ability to adapt to a changing and diverse environment where efficiency in management, leadership, as well as understanding the strengths and weaknesses of the organization’s risk tolerance are keys to survival (Schoemaker et al., 2018). Ultimately, to understand that an organization’s risk tolerance is inextricably tied to the conceptualization of the complexity of data transfer and how best to achieve the security of the data while processing, storing, and transferring the data to remain in compliance with cybersecurity policy, applicable standards, and government regulation is the key to ensuring secure cybersecurity practices (Calvard & Jeske, 2018; Hintze, 2018).

In a small business, the expanding landscape of vulnerabilities when obtaining new and improved technologies to maintain business relevancy and sustain growth is no different than in larger corporations; however, smaller firms must find innovative ways to maximize the buying power of every dollar through common sense cybersecurity strategies (Markey, 2018). As small businesses obtain state-of-the-art technologies, there are additional risks to the organization and its data transfer methods, including cloud computing, 5G technologies, and introducing IoT into the network (Au et al., 2018). The level of complexity in emerging threats increases the need for complex security strategies, thereby improving data security.

Technologies surrounding data transfer are rapidly changing, and information systems are in every aspect of society and culture as communications move from 4G to 5G (Kabalci, 2019). Data protection is a current concern of business leaders. Chaudhary et al. (2017) proposed strategies for building a secure data transfer system with burgeoning cloud-centric technologies that include the implementation of network service chaining (NSC), mobile edge computing (MEC), and software-defined networks (SDN). The apparent issue for small businesses is the cost of the technologies and the cost of implementation and training for these new forms of data communication that pronounce new and improved confidentiality, availability, and integrity measures (Berry & Berry, 2018). These new data communications and storage technologies also come with new payment structures packaged as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). Conversely, He and Zhang (2019) estimated that the training of cybersecurity analysts, who are already in high demand and often under-qualified, becomes an added expense for businesses that choose to apply the latest application of these services, thereby adding to the dilemma of whether to delineate a set of finite resources, take calculated risks in obtaining the new technology hoping it provides a return to remain competitive or remain one step behind business competitors. This reality also includes the possible necessity of maintaining these technologies, which may require contracts or the acquisition of a service technician to maintain the on-prem hardware and critical updates for the systems (Usman et al., 2019).

As businesses understand and become familiar with technologies such as SaaS, IaaS, and PaaS, other metrics are added to the cybersecurity hygiene of the organization, as symmetric and asymmetric encryption is highly recommended for the security of cloud-based systems (Lozupone, 2018). Researchers promoted data security that focuses on the user’s activities concerning data integrity, authentication, biometrics, and encryption controls as security strategies (Au et al., 2018). These strategies would appear to be a logical area of focus due to human error's number of data compromises promulgated. The inability to adequately identify the threat or the lack of adequate security and awareness training creates conditions conducive to data compromise. The conditions that persist for the threat to materialize consist of a motivated offender, a suitable target, and the lack of a capable guardian referenced through the lens of RAT, as posited by Cohen and Felson (1979).

Small Business Data Breach Concerns

Au et al. (2018) proposed that small business engages in varying forms of technology to remain competitive and provide a reasonable amount of due care in protecting customer-sensitive data by leveraging encryption as well as newer technologies such as cloud-based platforms that must be vetted to ensure companies that their platforms are secure. Maluf et al. (2018) posited that an attack could occur in an environment with adequate data security when an unauthorized motivated offender scans for vulnerabilities and weaknesses that can be leveraged to stage an attack. Potentially, vetting cloud-based platforms ensures that businesses are equipped with information that provides flexibility in adjusting their risk tolerance to prevent data breaches and determine the best security measures to protect and classify their data (Ali et al., 2018).

Today's advanced persistent threats (APT) pose a formidable challenge for organizations as these threats are specifically crafted to bypass the most sophisticated security measures (Cozzolino et al., 2018). Organizations that focus their attention on a single threat are not properly equipped with a strategic security plan that can adequately and efficiently respond to various evolving threats, resulting in mounting risks affecting the company’s credibility, expenses, competitive advantage, and efficiency (NIST, 2018). Small businesses’ issues are the resources needed to compete with larger companies as technologies are invented. As technologies are integrated into the small business and avenues for more significant revenue streams and efficient allocation of resources are created, small business leaders must be knowledgeable about the pitfalls that may affect their bottom line and compliance (Calvard & Jeske, 2018; Hintze, 2018).

Small businesses must now adopt and create a culture willing to try new and innovative strategies. Adopting a new culture can be achieved by starting at the top of the organization by providing cost-effective prevention methods to promote a level playing field when advancing security strategies. Technologies are redesigned and repurposed to be more efficient as these efficiencies are inevitable. The repurposing and redesigning of technologies also mean that the hackers are acquiring more sophistication in their methodologies, becoming more challenging to detect, costing businesses trillions in lost revenue in the future (Hou et al., 2018).

After highly publicized data breaches experienced by major corporations where millions of dollars in revenue and regulatory fines in the billions were lost, cybersecurity analysts adopted new strategies to counter cyberattacks known as “moving target defense” (Ghourab et al., 2019). Cybersecurity analysts adopted “goal protection” that, in essence, purposefully reconfigures the IT landscape to protect against identified attacks (Park et al., 2018). The methodology and strategy bare some insight into thinking outside of the box and utilizes a strategy that accounts for time, location, the motivated offender, and suitable target methodologies for identified threats that provide notable relatability to a newly formulated strategy in this study according to the concepts of RAT utilizing proximity and time as a strategy for data protection against external threats (Wen-qun, 2006).

Cybersecurity analysts have displayed resilience when the opportunity has presented itself due to the seriousness of the data breach events. Data breaches cost organizations substantial revenue and reputational harm, increasing their cybersecurity planning and resources (Gwebu et al., 2018). New and innovative cloud-based strategies that minimize vulnerabilities and protect against evolving threats can be beneficial in aiding small businesses in dealing with these costs (Liang et al., 2018). The vehicle (internet) that increases small businesses' attack footprint is a key in driving innovation, competitive advantages, and growth that centers around public and private security initiatives (Ding et al., 2018). Small businesses are an essential part of the nation's overall economy and are targeted disproportionately more than larger institutions (Small Business Association, 2021).

Cybersecurity analysts understand the seriousness of the threat which they face as the climate of data breaches and compromise of personal private information materialize; however, many small business owners listlessly regard themselves as not reaching the hacker's radar, thereby excluding the idea of any real threats to their organization despite the statistics creating a void in business cybersecurity strategies (Small Business Administration, 2018). The cost of adequately protecting customers' personal and private data increases as cybersecurity costs increase, creating concern amongst cybersecurity analysts and the companies that provide them with careers (Kaukola et al., 2017).

Without innovation and new ways of attacking this issue, small businesses will reach the point of unsustainability, as research has shown costs are expected to increase.

Small Business Resource Gap

The methodology that drives the protection of current systems, which hold billions of individuals' personal and private data, is based on traditional and likely unchallenged cybersecurity solutions (Sepulveda & Khan, 2017). These solutions are structured to prevent a host of threats from relying on outdated common vulnerabilities and exposure databases, which need to be updated daily to provide systems with adequate data to thwart current threats. The data is also utilized to devise a strategy to discover and remediate new and current vulnerabilities to protect network systems (Usman et al., 2019). Intrusion detection systems and its methods have been utilized to prevent common threats; however, the cost of providing this data, implementing the solutions, and maintaining these processes are of concern to small businesses (D'Arcy & Lowry, 2019). The concerns related to costs provide a pathway for new and innovative thinking about resource allocation and the outside-the-box application of strategies to protect small business network systems.

As newer systems are added to small business infrastructure, it is paramount that these new systems are carefully configured. The data derived from these systems are processed efficiently and managed responsibly (Laureani & Antony, 2019). This new infrastructure undoubtedly will require smaller businesses to make critical decisions on training for technical and security and awareness-based programs within their organizations (Humaidi & Balakrishnan, 2018). Security and awareness for small businesses can reduce the overall vulnerability landscape and motivate employees to feel part of the incident response effort. This reduction in the vulnerability landscape requires actively engaging others to improve cybersecurity and the overall development of security policies, thereby reducing the number of threats within the organization due to emails originating from external sources (He & Zhang, 2019).

Small businesses must remain forward-thinking in providing the most cost-effective strategies for confronting new and emerging cybersecurity threats. Paulsen's (2016) research is backed by Dawson et al.'s (2016) research that proposed that small business leaders can be flexible and ready to adopt new strategies to provide cybersecurity measures. By adhering to new and innovative thinking, small business owners are prepared to confront cyberattacks more effectively than their larger counterparts (Paulsen, 2016). An adequate security and awareness program can provide training that can save small business revenue by becoming aware of current threats to the organization and effectively reporting and engaging each of the threats, reducing the organization's exposure (He & Zhang, 2019). Providing training that makes employees aware of the cybersecurity requirements, thereby transferring understanding of the company's vulnerable infrastructure and its importance to the organization, can lead to a change in the culture and behavior of the organization (Humaidi & Balakrishnan, 2018).

The culture and behavior change can lead to new and innovative strategies for protecting the company's cybersecurity goals while providing cost-effective methods to decrease the overall cybersecurity cost of protecting personal and private customer data (Humaidi & Balakrishnan, 2018). The more cybersecurity analysts are engaged and provided with training to be successful may result in more significant dividends on the backend resulting in innovation and better protection of data as trained cybersecurity analysts will better understand the infrastructure, its threats, and how to apply effective strategies based on the current environment (Yoo et al., 2018).

External Cybersecurity Threats

Understanding External Threats

To provide a comprehensive approach to meeting the cybersecurity needs of an organization, it is essential to identify immediate risks as well as the risks that could cause the organization the most harm as a risk management strategy that involves surveying the landscape and identifying the common cyberattacks as well as cyber threats (Berry & Berry, 2018). To understand that IT is of the utmost importance to the facilitation of goods and services for all businesses, providing a strategy that addresses the risks associated with conducting business in a cyber environment can never be overrepresented (NIST Federal Resources and Coordination, 2019; Small Business Association, 2021).

Some of the most frequent threats to small businesses leverage several vulnerabilities inordinate to human nature to circumvent intrusion detection technologies and end-user training, such as utilizing a phishing email that delivers a malicious link (Qabajeh et al., 2018). The user unsuspectingly, due to a lack of proper training and resources, the small business, as articulated by Berry and Berry (2018), clicks the link that injects nefarious code into the browser taking the user to a malicious website where dangerous code, then delivered to the system bypassing all security controls and providing a command-and-control connection inside of the organization often called "drive-by downloads." Fellnhofer (2018) added that the exploit directly connects the unauthorized systems entering the network, unsuspectingly compromising confidentiality, availability, and integrity. This compromise of confidentiality, availability, and integrity leads to the small businesses experiencing an excessive number of losses due to reputational concerns, legal litigation by consumers who have been injured in the process, as well as the likelihood of governmental regulations and fines being rendered ((NIST Federal Resources and Coordination, 2019; Small Business Association, 2021).

The top cybersecurity threats to small businesses, where they incur the most significant financial hardship, consist of threats that include phishing or social engineering, ransomware, web-based attacks, malware, stolen devices, and denial of service attacks, respectively (Ponemon Institute, 2018). The statistics show that the greatest threats to small businesses are external threats. With the onset of COVID-19, organizations will continue to provide remote working options to meet the new challenges as these unforeseen circumstances have added to the attack footprint (Small Business Association, 2021). These new metrics will lead to the necessity of investing in new technologies and software solutions to ensure that employees can telework, as 54% of small businesses spent more on software solutions in 2020 than in 2019, and 75% expect the spending will increase next year (Small Business Association, 2021).

The new technologies and infrastructure will need to provide cost-effective strategies in applying cybersecurity to the growing attack surfaces and technologies

(Radziwill & Benton, 2017). This need for applied security in leveraging newer technologies invariably will increase the responsibilities of small businesses as there are limited resources and cybersecurity strategies designed for small business owners, further straining small business efforts (Berry & Berry, 2018). Information security and cybersecurity researchers argued that the ability of small businesses to create strategies utilizing comprehensive data based on mitigating cybersecurity threats and defending against cyberattacks is lacking (Gafni & Pavel, 2019). Small businesses' lack of resources does not allow the organizations to be well prepared for abruptly changing cyberenvironments that lack the personnel to understand the controls that should be implemented.

The lack of cybersecurity resources is also apparent, as well as the lack of trained cybersecurity analysts that understand how to provide a coordinated incident response effort and a plan of action that has been tested on a scheduled basis for readiness to effectively mitigate cyber threats (Osborn & Simpson, 2017). Young and Yung (2017) further described a lack of innovative strategies to maintain adequate protection against ransomware that emboldens hackers to exploit systems. In this scenario, a lack of a capable guardian, in the context of RAT, or a deterrent against ransomware threats are understood when a motivated offender and suitable target are present. Potentially the efficacy of the capable guardian is diminished.

Social Engineering/Phishing

As the research has implicated, social engineering attacks are significant threats to small business viability. They are some of the most challenging and costly to mitigate due to exploiting inherent weaknesses of the end-user and the deceptive tactics utilized to "hack the human" rather than the technology leading to compromised sophisticated cybersecurity systems. Fellnhofer (2018) asserted that the most significant threats are executed in phishing attempts and other deceptive, socially engineered measures that prey on human propensities. Jensen et al. (2017) also pointed out that phishing is a social engineering attack that utilizes deception to gain access to sensitive information to benefit the deceptive party. Jensen et al. (2017) identified the advancement of application testing to mitigate phishing attacks' success. Researchers have tested anti-phishing applications and have not fared well in preventing or mitigating susceptibility to phishing attacks. Fellnhofer (2018) proposed that security and awareness training would be a helpful tool for business leaders to provide an option that would reduce the attack footprint creating a more secure network environment. Jensen et al. (2017) argued that researchers have also instituted security and awareness training in conditioning the user to identify possible phishing attempts. Wolverton and Stevens (2019) acknowledged that some studies demonstrate that these are effective methods in mitigating susceptibility to phishing attacks; however, other studies have shown that one-quarter of the participants were just as susceptible to phishing attacks after receiving security and awareness training.

Understanding the threat of social engineering techniques requires an organization to present a united front amongst C-level executives to induce buy-in and promote security and awareness (Bada & Nurse, 2019; Hwang et al., 2017). The training is costly and not recognized as a practical and tangible return on investment for small businesses creating another expenditure that must be closely monitored and analyzed. Applying layers of security in the mitigation of social engineering techniques is warranted to improve small business cybersecurity defenses (He & Zhang, 2019).

Ransomware

Ransomware is “a type of malicious software that infects and restricts access to a computer until a ransom is paid” (US-CERT, 2020, para. 1). Ransomware is commonly distributed through phishing emails or “drive-by downloads” while appearing innocuous. They leverage a vector that exploits vulnerabilities in software (US-CERT, 2020). Ransomware is a credible and highly formidable threat to small businesses, and its tactics are relatable to social engineering or malware. Thomas and Galligher (2018) pointed out that ransomware is becoming the most prevalent form of malware attack for organizations that can also be deemed the most frequent form of extortion-based malware attributed to the cause of billions of dollars in losses globally. Small businesses must be proactive in mitigating these threats, which would entail creating and disseminating sound security technologies and protocols.

As reported by the FBI Internet Crime Report (2021), between 2013 and 2019, it is estimated at least $144.35 million in Bitcoin have been paid as ransomware ransoms, with the lion’s share of the attacks occurring in Texas in 2019. Richardson and North (2017) purported that the possibility of these attacks materializing and damaging a small business’s reputation and economic stability is very high. Small businesses, along with their larger counterparts, should provide a plan to deal with and decrease the effectiveness of the threat appropriately. In the face of these ranging threats, Forde (2017) articulated that small business owners looked at the threat landscape and decided, according to cost-effective strategies, that cloud-based technologies provided competitive price models in the face of growing costs. Richardson and North (2017) further noted that ransomware is responsible for millions of dollars in small business losses every year as technology increases in sophistication. Their ability to successfully circumvent the security of information systems while remaining undetected is apparent. Carr (2016) asserted that small businesses do not provide a robust and sufficient cybersecurity strategy, as this further exacerbates the concerns over a lack of cybersecurity analysts and resources.

Richardson and North (2017) noted that the utilization of cryptocurrency provides a secure option and is a key factor in these criminals maintaining anonymity while utilizing block-chaining techniques. This maturation in utilizing an obfuscation technique provides insight into the criminal element by utilizing cryptology techniques to cover criminal behavior and further create hurdles for small businesses when protecting their assets. Richardson and North (2017) further described ransomware as one of many external threats to small businesses, as ransomware would be understood as a subset of various threats that small businesses should be aware of. A small business may likely encounter many malware threats that compromise small business data systems on-prem. Advantages can be realized by creating honey pots to gain insight into the tactics and techniques of these threats; however, Näsi et al. (2017) argued that researchers expect to examine like qualities between spatial and antispatial routine activities research. In advancing the ability to detect new threats, these perspectives further incentivize small businesses to provide additional protection in creating effective cybersecurity strategies, threat analysis protocols, and proper logging regimens.

Web-Based Attacks

While various attacks threatened small businesses, the literature is clear on web-based attacks and their threat to small firms. Cheng et al. (2021) purported that one of the most significant cybersecurity threats remains the web attack due to its diversity in the type of attacks that exist under the moniker amid emerging technologies such as 5G, IoT, as well as cloud computing technologies (e.g., web-shells, sequel injection, and cross-site scripting). As a result, cybersecurity analysts utilized Hypertext Transfer Protocol Secure (HTTPS), secure shell (SSH), SSH File Transfer Protocol (SFTP), as well as other forms of encryption to protect their systems as cybersecurity has become a significant factor with the increase of internet utilization, information sharing, and IoT devices (Khan & Goodridge, 2019). Web-based applications provide essential functions and key services throughout organizations: e-mail, e-commerce, e-government, and social networking platforms.

Web-based applications contain PII and provide suitable targets for motivated offenders due to the ubiquitousness of the web-based application and the sensitivity of the data housed in the applications (Cheng et al., 2021). Small businesses must allocate resources to properly mitigate the threat of web-based applications due to the likelihood of the threat materializing and the impact of such a threat on business continuity. Traditionally, small businesses lack adequate resources and security and awareness training to effectively mitigate these threats (Ricci et al., 2019). The protection often comes in costly and sophisticated intrusion detection systems that include signatures that must be updated regularly.

Denial of Service Attacks

This type of attack utilizes various forms of malware to overwhelm a system with network packets exceeding several terabytes per second, leading to the termination of legitimate data requests overwhelming the system and consuming the compromised system's central processing unit, memory, and bandwidth with fraudulent data requests extinguishing services to the end-user (Chen, 2019). Many small businesses regard the denial of service (DoS) or distributed denial of service (DDoS) attacks as antiquated threats, or the impact and likelihood of the threat materializing don't warrant a threat that should consume much time, resources or effort due to a lack of availability of the tools utilized to execute a forensics analysis (Mansfield-Devine, 2015). In contrast, McDermott et al. (2019) found that DDoS attacks are more prevalent and more detrimental with the increase in IoT devices than in the previous history. With the ubiquitousness of IoT devices, more are becoming infected with botnets leading to higher DDoS attacks. However, Yadav et al. (2020) pointed out that denial of service attacks can render critical services of an organization inoperable, causing harm to the firm's ability to accept revenue and provide services while causing the complete isolation of the business from any communications, and is still regarded as a leading form of cyberwarfare. These challenges associated with a DDoS attack do not include the cost of recovery related to such an attack or entertain the risk of closure of the organization.

Small businesses lack the luxury of dedicated qualified cybersecurity professionals to adequately implement security measures, properly address and mitigate threats, and perform scheduled audits, translating into critical security tasks delegated to workers who lack the expertise to secure the organization, as identified by Berry and Berry (2018). A huge component in addressing the threat of DDoS attacks is leveraging the resources that include realistic data sets and test environments instituted for testing and research coupled with managing a set of finite resources (Koroniotis et al., 2018). McDermott et al. (2019) posited that the effectiveness of these attacks is directly related to the ability of this method of attack to go undetected while showing no signs of infection and evading experienced cybersecurity analysts. These factors demonstrate the reality that plagues small businesses and their viability. There are many residual effects of DDoS attacks on the organization, encompasses loss of consumer trust, which damages prospects and growth, the possibility of legal fees associated with lawsuits, having to provide credit monitoring fees for injured consumers, as well as a tarnished reputation that charges the organization with practicing lackadaisical business practices in securing sensitive customer data while demonstrating a lack of due care that could lead to federal regulatory fines as well as having a dramatic effect on operational costs (Chen, 2019).

Because of their stance, many organizations were ill-equipped to adequately mitigate such threats that led to the disruption of services of their internet-based division, leading to 32% of small businesses obtaining a third party to remediate the attack, as noted by Raineri and Fudge (2019). Berry and Berry (2018) articulated that recovery costs are regarded as significant when associated with small business owners reporting that the average cost of an incident equated to $20,000 per incident and as high as $38,000 to $44,000 in direct costs to the organization that encompasses Legal IT, public relations, and indirect costs of $8,000 for preventative measures. Bada and Nurse (2019) posited that small business has a finite set of resources, and without a risk management strategy, business impact analysis, as well as a mitigation strategy that incorporates threats, considering the likelihood, impact, and severity of each threat, can cause irreparable harm to the organization.

Cybersecurity Mitigation Strategies

Small Business Threat Mitigation

A valuable skill that qualified cybersecurity analysts possesses is identifying relevant threats and establishing a plan to mitigate those threats as the threat landscape changes effectively. Sharing these skills can provide valuable data for the culture of threat prevention. Bell (2017) noted that a synergistic and viable relationship that focuses on the shared information between private and government sectors is required to create initiatives that will aid in the prevention and mitigation of cyberattacks. Conversely, shared experience is valued in forecasting the threat landscape and understanding the cost of new technologies that protect the organization’s critical assets and the future mitigation of any threats to those assets to manage resources better. Kakucha and Buya (2018) posited that organizational personnel must understand their needs for cybersecurity and trust in systems that assure confidentiality, integrity, and availability. Given the importance of small businesses to the American economy, the government should consider a suite of low-interest business loans specifically to develop cybersecurity resources and infrastructure. Kisekka and Giboney (2018) articulated that with the risks associated with maintaining a business interconnected with ingress and egress systems, effective mitigation strategies are incumbent upon cybersecurity analysts and the effectiveness of data protection solutions identified by qualified cybersecurity analysts.

The fear of cyberattacks and the damages reported by organizations inextricably play a pivotal role in how organizations plan and implement cybersecurity strategies. Toch et al. (2018) pointed out that cybersecurity systems are ubiquitous and are even more commonplace due to the frequency of cyberthreats and government regulations. Cybersecurity has become the main component of all businesses. It is a critical area of concern when realizing risks to the organization's viability as an employee. Consumer PII is the most critical asset of each organization (Aishwarya et al., 2018).

The Small Business Association (2021) reported that small and medium-sized businesses employed 16.7 million people, including a ratio of 65% of all the nation's private-sector jobs. Gordon et al. (2018) asserted that an appropriate resource allocation strategy and smart investments in cybersecurity are critical to the viability of small and medium-sized businesses. Cybersecurity mitigation strategies should evolve as threats and government regulations develop and maintain a forward-thinking strategy to stay in alignment with the threat landscape and provide new and innovative approaches to cybersecurity threat mitigation. Cybersecurity analysts understand that an organization's greatest threat is compromising private, personal, and sensitive data.

Small and medium-sized organizations are bombarded with multiple threats daily, some of which go undetected as the loss of the administration of consumer data and company critical assets becomes a severe concern adding to the difficulty of protecting sensitive information, promoting innovation, and instilling confidence in data control of which is a reactive approach as noted by Yin et al. (2018). Inversely, utilizing a proactive approach, Mrabet et al. (2018) posited a cybersecurity strategy consisting of three tiers labeled pre-attack, post-attack, and attack, categorizing threats and providing engagement based on the determination of a phased approach was proactive. As we identify the growing concerns of a lack of qualified cybersecurity analysts within small businesses, innovation, and effective strategies are recognized, making a sizable difference. Chen et al. (2018) pointed out that human-centric cybersecurity research identified valuable revelations provided by collaborative and cognitive research within cyber operations; however, they ignored how the methods and outcomes of cyberattacks and government regulations affect human-centric cyberattacks results. In agreement with Selznick and LaMacchia (2018), Watad et al. (2018) articulated small businesses must understand that cybersecurity is regarded as a cost of participating in commerce and a requirement that deserves time and effort managing. Mithas et al. (2018) articulated a global shortfall of about seven million qualified cybersecurity professionals, which provides the impetus for small and medium-sized businesses to incur a lack of human capital to thoroughly research the broader issues that plague cybersecurity to increase security while lowering costs. The end game for small businesses is to adequately protect their stakeholders' interests by providing effective cybersecurity strategies while minimizing the legal risks to the organization.

People, Processes, and Technology

Part of an effective cybersecurity strategy is comprised of its leadership and the processes that are implemented with the technologies designed to protect the confidentiality, integrity, and availability of the organization and its critical assets. Karanja (2017) noted that uncompromising leadership usually consists of C-level executives who have experience making company decisions during a crisis and provide critical insights into security and governance procedures. Bauer and Bernroider (2017) further noted that senior-level executives play the most significant role in supporting the development and implementation of the cybersecurity program and its strategic purpose, which encapsulates policies and procedures created to protect organizational communications, assets, and systems from external as well as internal cybersecurity threats.

Small businesses are the main targets of cybercriminals as the likelihood of exploiting vulnerabilities within a system, which leads to data compromise translating into identity theft, is high (Qabajeh et al., 2018). Small businesses need to explore appropriate systems security approaches to implementing cybersecurity strategies that include mitigation procedures that are codified and implemented while consistently testing and updating processes. Grace et al. (2018) articulated that a review of internal controls processes plays a pivotal role in protecting systems, resources, information assurance, reliability, and accountability. Small business leaders can improve the efficacy of cybersecurity by implementing sound internal controls and a spatial component that deals with the accessibility of the systems as a new strategy. Furthermore, such innovations could lead to the initiation of a pragmatic approach and the procedural enhancement of the organization's cybersecurity policy in protecting critical data assets and information systems (Baldwin et al., 2017).

People, processes, and technologies are paramount in an organization as acknowledging these entities as integral parts of cybersecurity while allowing their input to feed strategic decisions within the organization leads to buy in creating a united culture that effectively utilizes a security and awareness approach to cybersecurity, significantly increasing the level of protection for critical assets within the organization (Clark & Guiffault, 2018). Sun et al. (2018) articulated that business owners must remain malleable, proactive, and mindful of changing cybersecurity environments and be willing and available to implement new technologies that strategically and long-term support the organization's viability. Implementing strategies to create an active culture would also involve qualified cybersecurity analysts who understand threats and actively provide innovative ideas to protect their organization to ensure cybersecurity is in front of an ever-changing threat landscape. Martin et al. (2017) further added that the balancing act consisting of technology, innovation, and growth is an ever-growing issue for small businesses; however, the mission is to continue identifying the salient risks and cybersecurity strategies to meet the demands of a changing cyberenvironment.

Incident Response

Wertheim (2019) articulated that incident response is often viewed as a cost center instead of a benefit to the organization that protects the bottom line. Executives share this culture and believe that incident response costs are better served by allocating funds to invest in time, money, and people who drive economic growth rather than optional response efforts. James (2018) noted that 95% of small businesses regarded cybersecurity as a critical function, but 45% did not report a structured approach. Furthermore, Schneider's (2018) study indicated that 80% of small businesses have no viable cybersecurity strategy. The lack of an incident response plan is primarily a problem in small to medium-sized organizations.

FEMA (2018) reported that 70% of all cyberattacks are aimed at small and medium-sized organizations. According to FEMA (2018), as much as 30% of those small to medium-sized businesses cease to exist after six months due to a cyberattack. In the United States in 2018, there were approximately 217,000 businesses whose revenue was identified as between $10 and $500 million, which translates into more than 65,000 of these businesses that can be expected to fail due to the economic consequences of a cyberattack. These unfortunate events have a devastating effect on society that equates to lost profits for other organizations and job loss for citizens.

NIST (2018) best practices dictated that organizations require a predefined plan of action to handle incidents in an incident response plan. An adequately staffed incident response team that includes stakeholders from all organizations and external partners is necessary to provide a layered approach to the defense and mitigation strategy to help protect business assets and critical infrastructure.

A well-developed incident response plan prepares the organization to pursue efficient response times and adequate procedures while carrying out attack scenarios and training drills, as purported by Greene et al. (2017). These tabletop exercises allow small business owners to identify vulnerabilities in the communication process and identify gaps in preparedness while strengthening the response teams' ability to carry out their duties under stressful circumstances. Greene et al. (2017) noted that the boards of directors require these valuable metrics and analytical data to determine if the organization mitigated the cyber threat at a practical level and followed the organization's IRP (incident response plan) drafted by the organization. Analyzing the data and metrics also allows management to assess their decision-making during the scenarios as alert business owners directly include leadership in the activities.

Incident response plans provide a practical approach to handling incidents in real-time while providing a system that records its weaknesses during the follow-up phase to create better response times as well as add efficiency in the process to better protect against future incidents. This approach to security is sorely needed for small businesses lacking a codified incident response effort.

Security and Awareness

Security and awareness are defined as the state of obtaining essential information regarding security policies and objectives within an organization (Bulgurcu et al., 2010). Safa et al. (2015) articulated that security and awareness play a critical role in forming acceptable behavior regarding security and awareness initiatives within an organization. Ngoqo and Flowerday (2015) also noted that the acceptance of the end-user to adapt to changes to security policy is determined by the level of knowledge the end-user possesses and the intended security behavior being adapted. He and Zhang (2019) further noted that organizations are better served by investing in cybersecurity training and awareness programs. It positively affects staff motivation to actively participate in the formulation of security policies to enhance employees' perception of cybersecurity and produce an agreeable outcome.

Small business resources are critically analyzed to ensure prudent decisions, and the resources are adequately allocated according to the threat landscape. Security and awareness implementation require training and patience before realizing the value of information security and awareness program. Korpela (2015) pointed out that the purpose of a security and awareness training initiative is to bring a security mindset to end-users alerting the culture to the dangers that plague information security assets while promoting the adoption of best practices that translate to another layer of protection for cybersecurity resources.

Security and awareness programs receive their budget after the report of significant data breaches that have surfaced in the news and the lack of adequate funding to make a credible difference in the security culture within an organization, as articulated by Lacey (2010). As Dhillon et al. (2016) further articulated, security and awareness programs promote the organization's values and provide a forum and a foundation for creating a knowledgeable and alert security culture while instilling an awareness of threats to the organization and identifying proper channels for prompt reporting. Security and awareness require a commitment from everyone throughout the organization to make a difference as everyone is incident response leading to a noticeable change in behavior (Humaidi & Balakrishnan, 2018). The time, money, and effort will be realized as the culture adapts to the new policies creating another layer of defense to protect organizational assets.

Policies and Procedures

Policies and procedures are additional layers that protect organizations from cybersecurity threats, vulnerabilities, and intended and unintended employee actions that can harm the organization. Karlsson et al. (2017) described a security policy as a directive that comprehensively executes tasks via single and shared goals. The directive is to achieve effective and reliable methods to complete the function.

Hwang et al. (2017) encouraged organizations to provide security education to their staff. It promotes self-responsibility, sheds light on the financial costs of security breaches, and helps organizations remain compliant while utilizing cybersecurity systems. Security strategies are instituted due to perceptions of threats that exist or are realized. Rothrock et al. (2018) relayed that most small businesses believed their organizations were secured correctly; however, the same small businesses were unaware that their security policies had been regularly updated. Rothrock et al. (2018) also pointed out that a belief amongst small businesses that persist is that they are consistently equipped to handle most threats rather than the idea that the need is to discover vulnerabilities within their environment.

Policies are most beneficial if reviewed every six months or at least every 12 months. According to Joshi et al. (2018), efficient management of security policies is better served when codified; a well-known IT governance policy is Control Objectives for Information and Related Technologies (COBIT), which aligns security principles that balance IT security strategy with the business environment. Patterson (2017) provided data from small businesses that relayed that input gathered from peers and budget shortcomings played a significant role in small business leaders' security choices. Patterson (2017) also pointed out that small business leaders seldom considered employees' positions when drafting security policies, as this action could have prevented the adoption of more effective cybersecurity strategies.

Liberal assessment, frequent monitoring of the technological landscape, and strategies are vital in providing a stable environment in the era of advancing cybersecurity threats, as posited by Goode (2018). End-users are the weakest link in an organization. George et al. (2017) pointed out that a security policy demands adherence to personnel behaviors inside and outside the organization, including C-level executives, as data compromise results from deliberate actions, inadequate security hygiene, or inadequate procedures. Strategies that govern behavior must be enforced throughout the organization to be effective and equitable.

New and Emerging Technologies

New technologies may prove advantageous for small businesses; however, this may also help cybercriminals leverage methodologies that can compromise the confidentiality, availability, and integrity of critical data within an organization. Zubiaga et al. (2018) confirmed that the introduction of new technologies provides an avenue for IoT devices to be added to the existing network infrastructure resulting in many advantages and process efficiencies as well as various concerns such as the compromise of personal data housed on the devices while connected to the network.

James (2018) confirmed that many organizations recognize that cybersecurity is key to the future of the viability of all businesses, as these organizations do not have an effective strategy to mitigate common threats. According to a study conducted by Schneider (2018), 80% of small businesses lack a cybersecurity strategy. Small business cybersecurity leaders should construct effective communication channels that alert the small business leaders of their threats in the future (James, 2018). Small businesses may start to address more effective ways of centralizing threat data to form policies and procedures based on current threats in creating new cybersecurity strategies.

According to Bell (2017), new ideas and strategies should be reviewed and analyzed by forming new relationships with the government and private sectors to contain and mitigate cyber threats effectively. In addition, organizations should formulate strategies that consider their risk appetite along with a business strategy that not only includes technology but carefully includes people and processes (Barafort et al., 2017). Radchenko et al. (2019) asserted that if cybercriminals compromise systems, it can result in a loss of revenue and cause significant harm to the brand. New tools are being offered that help organizations improve threat detection called security analytics (SA). This technology has opened pathways for new software, machine learning, and Artificial Intelligence (AI)-related techniques that include a broad range of capabilities (Lino et al., 2019). Greene et al. (2017) pointed out that it is prudent to include management in the organization's security activities when adopting new technologies.

AI is a relatively new technology that is now being leveraged in cybersecurity. The research community is often linked to machine intelligence as it is identified as an algorithm applied to machine learning. The technology has promising applications that are gaining in notoriety and impact securing systems positively; however, more research is needed to analyze the social and ethical concerns of applying the technology (Grosz & Stone, 2018).

According to Mithas et al. (2018), there are about six to seven million open positions for cybersecurity professionals; this equates to a lack of cybersecurity resources for all businesses but even more so for small businesses as they lack the capital to obtain the upper echelon of professionals available during this shortfall. Conversely, there is also a shortfall of foreign cybersecurity professionals. This concern provides an added dilemma as small businesses try to compete and maintain a qualified staff trained and experienced in applying current technologies to effectively understand how to mitigate new and emerging cyber threats by leveraging these new technologies. The introduction of AI into an organization usually results in a reduction in staff that would appear to be a positive result for small businesses stressing over resources; however, the lion's share of IT offshore work resides in India as they account for more than 70% of global consultants (Mithas et al., 2018).

IoT has been fully integrated into almost every network and introduces many issues due to a lack of IoT resources, as touted by Gupta and Quamara (2020). This integration of devices raises new concerns as the attack footprint has increased tremendously as only one compromised device is needed to breach a network (Hall, 2016). Studies have shown that added strategies can add complexity to network security. Each adaptation of a new strategy requires careful planning and identifying threats specific to the organization. Network security changes are better consumed when a rigorous training regimen is instituted as a strategy (Bryan, 2020). Concerning this study, the conceptual framework provides the impetus for adapting strategies that hinge on the availability of a suitable target, motivated offender, and the lack of a capable guardian. All must converge in time and space for a threat to materialize. The inference of complexity regarding targets or IoTs, motivated offenders, lack of a capable guardian, and the location or network of the compromise and its anomalies requires further investigation.

Safa et al. (2018) agreed that management should consider environmental factors that motivate users to breach the confidentiality, availability, and integrity of data systems. If management is not on board and at the table for these new strategic initiatives, the lack of support could quell progress in providing new and emerging strategies to mitigate threats (George, 2016).

Cybercrime as it Relates to Time and Space

In reviewing strategies that are not identified as the industry standard**,** the correlation between physical crime and cybercrime must be understood as the difference between cybercrime and traditional physical crime is not the level of complexity associated with the incident but the environment in which it occurs that provides factors to determine the root cause (Miró-Llinares & Johnson, 2018).

When exploring newly combined strategies to prevent cybersecurity threats, researchers will do well to provide a solution that is economical and can be used liberally across small businesses without causing added financial hardship furthering the gap of unaffordability of new technologies leading to a degradation in providing capable guardianship as well as the prevention of data compromise. Felson and Eckert (2019) pointed out that it is key to demystify cybercrime concerning a physical crime to properly study preventive measures and their added dimensions. This study of the added dimensions attributed to physical aspects of a crime will likely be essential to small business cybersecurity analysts in creating strategies that effectively protect and mitigate cybersecurity threats. As reported by the Internet Crime Complaint Center (2018b), the few statistics found on the impact of cybercrime show that the less technical vectors that facilitated the compromise caused more victimization, as well as financial losses; therefore, this strategy is essential in the prevention of cybersecurity threats as in comparison to physical crime.

The parallel exists in cybercrime which includes the human factor and is often overlooked regarding data breach prevention. As P.J. Brantingham and Brantingham (1981) proposed, environmental criminology was formulated to provide an out-of-the-box approach to crime prevention solutions that were not applied through conventional criminology frameworks. The focus was on the motivated offender. Its primary focus was unambiguous, shifting the analysis from the motivated offender to the situational spatial environment in which the crime took place.

The strategy was posited by Jeffery (1971) in response to research regarding findings that there were no effective means to rehabilitate motivated offenders in the criminal justice system (Martinson, 1974). This strategy of applying out-of-the-box solutions can only provide another level in which cybersecurity analysts can use additional strategies that are cost-effective, as they only require crime analysis to implement the strategy, which shifts the focus from the motivated offender, of which we have very little to no control of, to the environmental factors upon which the crime takes place, of which we have total administrative authority, that translates into the networks that house the PII and employee data. Implementing such a strategy will require applying a conceptual framework and cybercrime analysis tools that must form an interdependent relationship to increase their functionality in eliciting the identification of commonalities shared across physical and cybercrimes.

Transition and Summary

In Section 1, I provided context for the problem statement, purpose statement, the introduction of my research questions, and the supporting interview questions revolving around utilizing a finite set of small business resources. Emphasis was directed to the analysis of strategies that provide cost-effective methods to address potential cyberattacks allowing small businesses to have a battery of less utilized strategies to secure their environments. I applied a host of definitions that are referenced in this study and explained the limitations, delimitations, and assumptions that apply to the context of this study. I have further demonstrated that repackaging a set of strategies could prove beneficial in creating more secure environments for small businesses.

The impetus was placed on leveling the playing field when needed resources were scarce and lowering the attack footprint against motivated offenders. In reviewing the professional and academic literature, I provided a lens that leveraged Cohen and Felson's RAT and new and innovative strategies posed by Wen-qun, which solidified this study's foundation. The literature review provided context and closed gaps in the virtual crime versus physical crime construct. I discussed topics that provided context for cybersecurity, threat mitigation, new and emerging technologies, cybercrimes related to time and space, policies and procedures, incident response, security and awareness, and people processes and technologies. The literature review culminated with discussing cybercrimes related to time and space, delving deeper into less often applied strategies that may be very useful in application to small business cybersecurity.

In Section 2, I identify methods for executing the study that include the researcher's role, participants, ethical considerations, data collection methods, and other crucial elements and salient points regarding applying the study's findings. In Section 3, I provide a holistic view of the study, a presentation of the results, an application to professional practice, the implications for social change, recommendations for action, suggestions for further study, reflections upon my experiences conducting the study, as well as a research conclusion of the varied research of this study.

Section 2: The Project

This section contains information covering the researcher's role, participants, sample population, and the research methodology and design. I provide justifications for my approach regarding the ethical considerations of the study, data collection techniques, and reliability and validity.

Purpose Statement

The purpose of this pragmatic qualitative inquiry was to explore the strategies utilized by IT cybersecurity analysts of small businesses to prevent external cybersecurity threats. The target population included nine IT cybersecurity analysts from small businesses located in Texas who have successfully implemented strategies to prevent external cybersecurity threats. The findings from the research could potentially affect social change by empowering a cadre of cybersecurity analysts to engage in the application of innovative small business strategies to prevent cybersecurity threats.

The analysis of cybersecurity strategies in practice, such as geospatial techniques and tactical decisions to reduce domestic cybercrime adopted into a virtual environment, could potentially provide the application of methods and strategies in new and innovative ways to affect social change leading to more secure small business cybersecurity environments. A more secure cybersecurity environment translates to increased valued resources for small businesses and their bottom line. The potential increase in economic capital provided by applying these strategies could lower the small business attack footprint translating into more resources being allocated for job creation, improved data protection services to protect employee and customer data, and job training for those seeking gainful employment, leading to greater economic stability for the nation.

These strategies could provide a model for small businesses to effectively maintain secure network environments without considerable increases in budget and changes in resource allocation strategies, which would allow small businesses to compete with their larger counterparts consisting of ample research and development budgets. Providing a model to secure small business network environments adequately creates a path to establish a customized group of services for consumers and provides a solution to obtain highly trained cybersecurity professionals more readily.

The study's population is appropriate because IT cybersecurity analysts institute the strategies and evaluate the resources utilized to prevent cybersecurity threats. For this study, a small business was defined as an organization that employs fewer than 500 employees (Small Business Administration, 2019). In this study, the positive social change implication includes the potential for decreasing the compromise of personally identifiable, confidential, or sensitive customer information at its core and improving the human condition. More so, the enhancement of cybersecurity strategies in small business organizations may provide a better allocation of finite resources through a demonstrative set of innovative methods that aid in formulating techniques and strategies to prevent the compromise of personally identifiable customer information.

Role of the Researcher

In choosing a qualitative method, the researcher is the primary data collection instrument, and the role of the researcher is regarded as equally important to the study as the participants upon which their rich input is deemed to be of paramount importance (Yin, 2018). The role of the qualitative researcher is immersed in the repetitive nature of gathering and analyzing data from the participants, remaining objective about the research outcomes, and identifying trends to initiate further inquiry. Following these protocols provides context for better identifying themes and reporting them honestly at the behest of discovering contrary outcomes to preconceived notions about the research problem, according to Fusch and Ness (2015). Yin (2018) noted that there exist prerequisites to understanding the issues that may be mitigated to enhance the validity and reliability of the study.

In my role as the qualitative researcher, I used strategies to minimize risks to research participants. Bartlam et al. (2018) posited that participants are not inextricably tied to the researcher. The rigorous process can be morally challenging due to the personal and repetitive nature of the inquiry throughout varying levels of the study.

The topic of cybersecurity is a familiar one concerning the amount of experience I possess in the field, academia, and practice. My professional experience as a director for the School of Graduate Studies in Cybersecurity equips me with a global perspective on the profession’s issues. I have also held the role of the research participant as a senior cybersecurity engineer in Texas. My varied experience can be seen as a pro and a con. On one hand, I have a unique perspective on the research problem. I have dealt with the dilemma daily for a better part of my career, critically thinking about adopting strategies to mitigate some of the concerns. On the other hand, the amount of experience can lead to tunnel vision and impede a truly objective solution to the research problem. Controls were instituted to mitigate biases that may affect objective outcomes and recommendations for future studies.

The researcher's role involves engaging the study ethically and remaining compliant with the Belmont Report research protocol. Pearce et al. (2018) noted that the *Belmont Report* consists of ethical guidelines and principles to adopt when researching human subjects. Ross et al. (2018) also posited that per the *Belmont Report* protocol, the researcher's responsibility is to insist upon and adhere to moral obligations to provide respect for persons, do no harm, and provide justice in dealing with human subjects. Palmas (2018) further articulated that the *Belmont Report* provides an ethical frame of reference for the conduct of researchers when engaging human participants. Reid et al. (2018) additionally asserted that the *Belmont Report* protocols provide respect for others, ensuring that all human participants have freedom of choice in making independent decisions. Leiber et al. (2018) further noted that the adherence to justice outlined in the *Belmont Report* protocols is the premise of equal treatment of all human subjects. I strictly adhered to the *Belmont Report* by engaging in the avoidance of impartiality when selecting participants, respecting respondents, and maximizing the benefits of the study while minimizing risks to all participants.

In the realm of mitigating biases, Yin (2018) clarified that it is the responsibility and moral obligation of the researcher to adhere to the highest protocols of research, provide candid data, avoid any forms of deception, and accept the responsibility of cultivating their work product. In essence, in mitigating potential biases, the researcher has to remain the data collection instrument and not disengage from the research (Fusch

& Ness, 2015). To avoid biases and conflicts of interest, I selected participants with whom I had no past or current relationships. Kache and Seuring (2014) articulated that researchers mitigate biases by selecting participants with no prior knowledge or previous history. As an additional mitigation control to the effects of bias, I maintained strict adherence to a planned interview protocol and remained attentive to any adverse reactions that may have developed during the semistructured interview process. Fusch and Ness (2015) asserted qualitative researchers must be mindful of their lens according to their worldview and how their view shapes the interpretation of the data to interpret the participants' behaviors effectively.

According to Yin (2018), a researcher must ensure validity and integrity and strictly adhere to the protocols when conducting interviews to mitigate biases when collecting data. The rationale for conducting semistructured interview protocols is to limit occurrences of bias. I focused on the interview questions (see Appendix A), anticipating rich responses to the research questions. The focus of the semistructured interviews was to elicit information regarding the analysis of cybersecurity strategies to prevent external cybersecurity threats. Yin (2018) touted that the researcher should understand that any beliefs, prejudices, expectations, and cultural values could affect the study's outcome.

For this pragmatic qualitative inquiry, I gathered data from cybersecurity analysts primarily involved in resource allocation, threat mitigation, and threat detection. I reviewed the organizations' businesses and social media pages to identify possible gaps in the organization's security posture or identify overlooked vulnerabilities via passive reconnaissance. I provided an interview protocol (see Appendix B) that contains directions and guidance that I did not deviate from when conducting interviews. The utilization of the semistructured interview protocol ensures that the integrity of the interview process will not be compromised. The interview process was scripted to provide comprehensive coverage of the data and elicit rich themes and interactions from each research participant.

Participants

A prerequisite of the participants for a qualitative study is to experience the phenomenon, as this observation was asserted by Yin (2018). Fink (2000) also posited that participants are often selected based on their familiarity and experience with the topic when executing a qualitative study. The participants' perspective is funneled through the research question's lens to provide detailed descriptions of the research topic (Draper, 2015). I did not engage in a pilot study, as the theme development was derived from nine participant interview transcripts, industry-standard documentation regarding the NIST SP 800 series, NIST Cybersecurity Framework (CSF) documentation, International Standardization Organization (ISO) 27001, as well as notes derived from participant interviews concerning current cybersecurity prevention strategies to provide multiple sources and provide greater validity for methodological triangulation as posited by Yin (2013). The sample for this study consisted of nine IT cybersecurity analysts working in Texas who have displayed the ability to adequately protect their organizations from external cybersecurity threats during their tenure. Moustakas (1994) further posited that when conducting a qualitative study, the researcher should obtain participants who possess the knowledge and expertise to provide rich responses to research questions adequately. I executed the data collection process after receiving confirmation from Walden University's Institutional Review Board (IRB). I utilized snowball and purposive sampling to engage and recruit research participants. Yang et al. (2018) articulated that it is critically essential to index resources and leverage the expertise of a small set of participants when gathering research data.

I explored strategies utilized in practice to protect and maintain the security posture of the organizations that touted no significant data breaches. Northrup and Shumway (2014) further noted that participants must provide knowledgeable aspects and perspectives derived from experiences about the phenomenon in qualitative research. Following the research protocols, I identified potential research participants who meet the criteria and possess the prerequisite knowledge to provide informed answers to the central research question in this study. I selected nine cybersecurity analysts who meet the eligibility criteria for research participants in this study. The eligibility criteria for this study consist of cybersecurity analysts from small businesses in Texas who implemented strategies to protect their organizations from external cybersecurity threats.

I leveraged LinkedIn and additional social media platforms to recruit and engage participants. Brown and Danaher (2019) articulated that it is advantageous for the researcher to build a rapport and establish trust with each participant when executing a semistructured interview process when utilizing a qualitative method. Prior (2017) also demonstrated a rapport as the participant and the researcher shared relatable responses during the semistructured interview process. Latkin et al. (2016) argued that the researcher and participant must be mindful of moments when building rapport and trust, as bias can show when both the researcher and participant reveal similarities and what appears to be shared beliefs within the study. LinkedIn has been regarded as an effective and efficient way to identify the small business with which each participant is associated and their positions within these organizations. After identifying the eligibility criteria for each participant, I emailed each participant a consent form that serves as an invitation letter that provides a brief context for the study, along with a request for a reply. After reviewing the consent letter, if they were interested in becoming a participant, they were instructed to reply, “I consent,” which would indicate their willingness to participate in the study. Providing background related to some of the experiences I have encountered was an effective measure to establish a rapport and build trust with participants (Nadal et al., 2015). I established a rapport that centered around the research question and how they see the problem within their organization. I utilized videoconferences through Zoom (https://zoom.us) to allow participants more flexibility in setting a time and location for the interview, which allows the participants to engage in a comfortable setting while still maintaining privacy (Yin, 2018).

Research Method and Design

Research Method

I considered three types of research methods: mixed-methods, qualitative, and quantitative. When applying methods to research questions, I selected the qualitative method as the most appropriate methodology for this type of study. The qualitative method effectively elicits rich responses to how and why questions (Ponelis, 2015). Although the quantitative method is very effective when evaluating a stated hypothesis and elucidating findings via the utilization of inferential statistics (Spicker, 2018), the quantitative method was not appropriate for this study as that method hinges on a hypothesis to provide data to support the study. A mixed-methods approach was not feasible for this study as it requires comparing relationships or differences between variables, which is not the premise of this study. Yin (2018) articulated that a mixed-method approach is most appropriate when correlating participants' experiences and empirical data to examine relationships and elucidate variables. Latunde (2017) indicated that the qualitative research method allows for practical examinations of limitations and strengths while highlighting the salient points of the study. Matt et al. (2017) asserted that qualitative descriptions are essential when elucidating changing processes. I leveraged the qualitative method to explore organizational strategies of cybersecurity analysts from small businesses to prevent external cybersecurity threats. In utilizing this method for this study, I logged data via interviews, a review of social media sites, and the obtained documents.

Research Design

Qualitative research designs incorporate many possibilities when engaging in a research study. The potential designs include phenomenology, ethnography, the Delphi technique, pragmatic qualitative inquiry, and case study designs. I considered a pragmatic qualitative inquiry, a phenomenology, and an ethnography. After reviewing these qualitative research designs, I decided that the pragmatic qualitative inquiry was the most appropriate qualitative research design for this study. The driving force of this study was to provide a pragmatic approach to exploring small business cybersecurity analysts' strategies utilized to prevent external cybersecurity threats. The design approach is warranted because this study involves the emergence of innovative strategies that could be applied to current practices. Savin-Baden and Major (2013) articulated that the most appropriate design for linking theory and practice was the pragmatic qualitative inquiry. Leedy and Ormrod (2015) noted that when utilizing a pragmatic qualitative research method, the researcher intends to present a complete description of a phenomenon within a specific context in a real-world setting, allowing a liberal amount of flexibility in methods and techniques applied to understanding a not yet understood phenomenon. As I explored current cybersecurity strategies, new and innovative applications were applied and analyzed in conjunction with practical methods to form a new set of strategies. Applying these innovative strategies to engage further the possibility of increasing the effectiveness of current mitigation methods while lowering the attack footprint at very little to no cost to small businesses could prove advantageous in securing small businesses' resources leading to increasing their bottom line.

In ethnography, the researcher is inserted into the participant's cultural group environment. The researcher attempts to understand better the participants' behaviors (Watson, 2018). Kassan et al. (2018) posited that the researcher is an intricate participant group when utilizing an ethnographic design. In utilizing an ethnographic approach, the researcher aims to take on the environment of the study participants to gather data on specific cultures, norms, or customs to gather data about behaviors. Ethnography would not have been an appropriate design for this study as this study requires rich inquiry to understand the phenomenon that plagues small businesses and not the participants' behaviors.

Phenomenology is based on a descriptive perspective, wherein the participants provide a detailed description of the core experiences while engaging the phenomenon by referencing the topic under discussion (Adams & van Manen, 2017). The phenomenology design leverages the intent to explore how participants interpret the topic under study and the lived experiences in the context of the phenomenon (Adams & van Manen, 2017). Researchers who utilize the phenomenological design execute interviews to identify common themes among experiences (Gill, 2014). The phenomenological design would have been appropriate for this study if the focus was on the topic of the study rather than the lived experiences in reaction to the phenomenon. Given that the focus of this study was to explore cybersecurity strategies of small businesses to prevent external cybersecurity threats, the phenomenological design was not appropriate.

Data saturation is reached when there is no new data being provided. When there is ample information to replicate the study and further coding does not remain a possibility, data saturation is reached (Fusch & Ness, 2015; Lowe et al., 2018). Ando et al. (2014) also pointed out that data saturation occurs when the possibility of eliciting new themes or codes is not achievable from the data collected.

In this pragmatic qualitative inquiry, data collection occured through nine participant interview transcripts, industry-standard documentation regarding the SP 800 series of the NIST, NIST CSF documentation, ISO 27001, as well as notes derived from participant interviews concerning current cybersecurity prevention strategies. The participants engaged in this study included nine small business cybersecurity analysts who completed an online semistructured interview via Zoom (https://zoom.us) containing 10 open-ended questions. Participants engaged in in-depth dialogue that provided greater detail on the questions and any additional questions derived from the in-depth participant responses.

Population and Sampling

The population for this study consisted of small business cybersecurity analysts that utilize strategies to prevent external cybersecurity threats in Texas. Alase (2017) posited that researchers should engage at least five research participants who have all experienced phenomena leading to the interrelationships of participants' experiences, which can be documented and interpreted**.** I utilized snowball and purposive sampling to recruit nine cybersecurity analysts of small businesses to engage participants whose organizations successfully prevented external cybersecurity threats. Robinson (2014) instituted an approach to snowball sampling that provided steps that consisted of (a) describing the criteria of the sample world, (b) determining the sample size, (c) constructing a sampling method strategy, and (d) defining the source of the sample. A purposive sample of nine cybersecurity analysts, until data saturation was reached, who successfully implemented cybersecurity strategies to prevent external cybersecurity threats participated in online semistructured interviews containing open-ended questions from this cadre of professionals.

Yin (2018) noted that the sample size depends upon the sophistication or complexity of the research topic and the depth and breadth of the data gathered. Gentles et al. (2015) also asserted that the sample size might consist of between 4 and 15 participants to reach data saturation within a qualitative study. Cleary et al. (2014) further clarified that it is essential to document that generating the focus on the data regarding the research question is required in direct correlation to the sample size of the participants to reach validity and saturation. Walters (2017) executed a qualitative study within a financial services organization to explore strategies businesses utilize to recruit cybersecurity professionals leveraging a sample size of five financial services organizations. Saber (2016) executed a qualitative study of small businesses to collect data from five small business leaders to analyze cybersecurity strategies. As my research study is comparative in design and method to the research conducted by Saber (2016) and Walters (2017), I engaged nine cybersecurity participants until data saturation was met, with various sources of data collection as an appropriate sample size in performing this qualitative research study.

The theme development was derived from semistructured online face-to-face interview responses, relevant NIST documentation, and additional industry-standard documentation concerning current cybersecurity prevention strategies to provide multiple sources and added validation for methodological triangulation, as posited by Yin (2013). Eligible research participants for this pragmatic qualitative study are cybersecurity analysts from six small businesses in Texas who implemented strategies to prevent external cybersecurity threats. I have conducted semistructured Zoom (https://zoom.us) video conferencing interviews with research participants, as semistructured interviews took a myriad of forms that consisted of email, webchat, face-to-face, and telephone, as posited by Brown and Danaher (2019). The interviews took place in the convenience of the interviewees' homes or offices and consisted of about 45 to 60 minutes in duration, with appropriate follow-up meetings of about 20 minutes when data saturation was not reached. I did obtain informed consent to execute interviews and obtain authorized access to any personal documents (see Appendix B) relevant to providing data applicable to the research question through cybersecurity analysts of the organization. I did present the context of the study via email. The participants received an invitation via email to take part in face-to-face Zoom (https://zoom.us) interviews. I concluded the interviews by requesting documentation applicable to the research study (see Appendix B).

Once the organization was identified, the purposive sampling method ensured that I recruited cybersecurity analysts with expertise and assurance that they were experts in the field. Snowball and purposive sampling were utilized to identify participants who met the established perquisites for the study. Mohr and Metcalf (2018) posited that the purposive sampling method allows a researcher to create specific timelines with a high probability of timely competition utilizing data elicited from businesses. Elo et al. (2014) noted that purposive sampling is appropriate when the research participants possess the requisite knowledge of the topic and the phenomenon for a qualitative study. From this purposive sample, nine cybersecurity participants have engaged in semistructured interviews via Zoom (https://zoom.us) video conference discussions that reached data saturation.

Mohr and Metcalf (2018) also articulated that data saturation is reached when no further data can be derived from the research participants to inform the study. Saunders et al. (2018) further articulated that data saturation involves justifying the amount of data gathered as equal to the data required for research. Data saturation was achieved by interviewing participants to exhaust all information applicable to the research questions, and no new data could be collected. Data saturation was determined by analyzing participants' responses in real-time during the interview while formulating new questions as participants revealed salient points, norms, and constructs regarding the research topic. The purposive sample was sufficient to reach data saturation as no new data could be derived from participants' responses.

Ethical Research

Yin (2018) articulated that during several phases of research, the qualitative study requires ethical standards in designing and researching the study. The ethical standards would also apply to any ethical issues about participants' sensitive information. Eisenhauer et al. (2019) further articulated that engaging in ethical research practice requires the acquisition of voluntary participation and informed consent from each research participant. Yip et al. (2016) further noted that it is incumbent upon the researcher to protect the confidentiality and privacy of the participant. When engaging each potential research participant, I explained the interview process to each participant to ensure that each participant was comfortable with the nature of the study and the subject matter before presenting an informed consent form for each participant's signature. In contacting each participant, I provided an "informed consent form" along with documentation that outlined the purpose of the study and included any foreseeable risks or benefits of the study. I outlined any study conditions, such as the intent to record each participant's interview. As the condition exists to record any research study participant, I also clearly communicated these conditions to each participant at the start of each interview. All potential research participants were required to respond to the introductory email outlining the nature of the study, its conditions, as well as foreseeable risks or benefits of the study, including a consent form. There were no incentives for participants to engage in this study as the conditions of the study strictly adhered to informed consent preceding voluntary participation. Due care ensured that the research was conducted ethically while adhering to the highest research standards outlined by the university's ethical guidelines and continually adhering to the highest academic research practices.

The IRB bears the responsibility of overseeing human studies research while ensuring that the study that the researcher conducts is per generally accepted ethical standards that adhere to state and federal regulations and university procedures and policies (Caldamone & Cooper, 2017; Qiao, 2018). I obtained the Walden IRB approval before collecting data and engaging participants (Approval no. 05-11-22-0517128). I instituted the informed consent process that required participants to sign an informed consent document that outlined their rights as research study participants that included a method for withdrawing from the study. At any point in the ethical research process, if any participant was uncomfortable with any part of the process, their right to withdraw was respected. No further engagement ensued as outlined. The process for withdrawal from the study consisted of participants informing the researcher that they would like to abstain from any further participation in the interview process. Once it was communicated to the researcher that the participant declined to engage in the research study, they were removed from the research process (Nadal et al., 2015). Any documentation was purged from any document collections with no further participant engagement. No form of repercussion existed for any organization or individual participant when exercising their right to withdraw. Participants of the study have anonymity achieved through Zoom interviews conducted at the participants' undisclosed venue of choice, as outlined in the consent form, adhering to the participants' right to privacy concerns. Participants were required to maintain a level of confidentiality for the study that required the participant to abstain from discussing the names of the individuals who took part in the study and any content of the interview with any outside parties while the study was being conducted. Due care was exercised, and all ethical guidelines established by the university were followed to ensure all participants and organizations were protected from any harm because of participation in the study.

In the interest of performing ethical and confidential research as outlined by the policies and procedures of the university, the names of the organizations and individual participants were masked in the study documentation. I maintained an Excel spreadsheet with the names of individual participants and organizations participating in the study and assigned generic names to each entity (ex., organization I, organization II, participant I, and participant II). The Excel spreadsheet and NVivo 12 software was the only documentation where any names were tied to the organizations and research participants in a manner that was anonymized, further protecting the privacy rights of each entity. The Excel spreadsheet resides in an encrypted format housed in a OneDrive folder, as no other copy of the documentation will exist. The process and manner of storage of the documentation for the study ensure an audit trail exists and a codified method of referring to each organization and individual participant in an anonymized manner throughout the research study.

In strict adherence to the Walden University research process, data from the research study will be maintained in an encrypted anonymized format for no less than five years after the study has been completed. I faithfully maintained the encrypted format of the anonymized research documentation housed in a OneDrive folder for the duration of the five years. Upon the end of no less than five years, all data associated with the study will be destroyed following any policies and procedures outlined for the method and environmental safety measures suggested for its destruction.

Data Collection

Data Collection Instruments

The researcher is seen as the pragmatic qualitative inquiry's primary data collection instrument, as noted by Clark and Vealé (2018). Yin (2013) also noted that the researcher is the primary instrument for gathering data. In this study, I conducted the data collection as the primary data collection instrument utilizing an online semistructured face-to-face interview. The methodology for data collection in this study has been chosen to elicit a more rich and more diverse set of data points to provide greater insight into the research topic for data analysis. I did not engage in a pilot study. The theme development was derived from semistructured online, face-to-face interview responses, relevant NIST documentation, and additional industry-standard publications concerning current cybersecurity prevention strategies. Yin (2013) purported that methodological triangulation of interview data can be better achieved with various sources and methods to elicit a greater sample of data from several perspectives. Small business cybersecurity analysts of nine participants answered ten open-ended questions (see Appendix A) in an online interview format as instructed by Elo et al. (2014). Graebner et al. (2012) also articulated that open-ended questions elicit responses that allow participants to share thoughts and detailed experiences. The ten open-ended questions were formed leveraging the lens of Cohen and Felson's (1979) RAT.

As the interview process was conducted, nine small business cybersecurity analysts indicated that they had completed the online review of the document that addressed the specific business problem, preceded by the acceptance and signage of the Informed Consent Form. I consistently executed each interview by adhering to the interview protocol (see Appendix B) as outlined while maintaining consistent and effective note-taking and attentive observation of participant responses during each interview. In maintaining reliability, the researcher must prepare and adhere to the same document completion process throughout the research steps and procedures to minimize error and bias (Kihn & Ihantola, 2015).

A subset of nine cybersecurity participants has engaged in semistructured Zoom (https://zoom.us) interviews to obtain additional data regarding the strategies of nine small businesses' cybersecurity analysts to prevent cybersecurity threats. I also analyzed relevant NIST documentation as well as other industry standard documentation that were relevant. A review of these documents was possible via Google searches as well as the industry standard NIST website. When conducting interviews, Berger (2015) articulated that the researcher must remain unbiased, eliminating preconceived notions regarding personal characteristics such as gender, race, personal experiences, or political beliefs. An engagement of the subset sample of nine participants was conducted until data saturation was met via semistructured Zoom (https://zoom.us) interviews. There were informative data collection sessions in which small business cybersecurity analysts were asked to elaborate on the initial ten questions. The online semistructured interviews provided a forum to elicit in-depth descriptions of the selected questions and any additional questions derived from participants' responses. The semistructured online Zoom (https://zoom.us) interviews were leveraged to elicit detailed thoughts and experiences on MTD defense strategies seldom utilized in cybersecurity domains. After the interview process had concluded, I requested any documentation of cybersecurity strategies to prevent cybersecurity threats from gaining a foothold on the organization's network (see Appendix B).

Industry standard documents were analyzed to ensure that multiple data points were included in data collection and methodological triangulation points to strengthen the study's validity, as posited by Yin (2013). Yin (2018) further articulated that a myriad of effective data collection methods may include evaluation, note-taking, interviews, peer-examination, as well as digital recordings. The primary objective of data collection instruments was to elicit participants' viewpoints and opinions regarding cybersecurity strategies to prevent cybersecurity threats (Khan, 2014). Through a rigorous analysis of the data collection provided in the participants' responses, I provided the efficacy of cybersecurity strategies within small businesses.

Pozzebon and Rodriguez (2014) articulated that the validity and reliability of the data collection instrument are paramount in the execution of qualitative studies to minimize subjectivity and biases. When demonstrating the reliability of a qualitative study, the same data collection methods can be repeated by another researcher that will obtain the same results (Pozzebon & Rodriguez, 2014; Yin, 2013). To obtain reliability in this pragmatic qualitative inquiry, I ensured the documentation of all procedures and research steps and validated that the research design and method remained consistent throughout the study. Elo et al. (2014) articulated that the exactness of the findings, as defined by the participants and researchers, is paramount when adhering to validity.

My abbreviated interpretation of transcripts responses to the 10 open-ended questions was provided to each study participant to confirm accuracy. Yin (2018) posited that member checking is a crucial aspect of qualitative research to examine the validity and accuracy of the data provided by the participant and aid in the elimination of biases. Thomas (2017) further posited that accuracy for the researcher and the accurate representation of a participant's viewpoint is provided when member checking is performed and no new information can be derived. Participants engaged in the semistructured Zoom interviews received my interpretation of their responses, allowing each participant to perform member checking, leading to the confirmation of accurate comprehension of the interview responses.

For this study, the data collection process consisted of semistructured online, face-to-face interview responses, relevant NIST documentation, and additional industry-standard publications concerning current cybersecurity prevention strategies. I did not engage in a pilot study. The theme development was derived from semistructured online, face-to-face interview responses, relevant NIST documentation, and additional industry-standard publications on current cybersecurity prevention strategies to provide multiple sources and added validity for methodological triangulation. Yin (2013) purported that methodological triangulation of interview data can be better achieved with various sources and methods to elicit a more significant sample of data from several perspectives.

The first phase of data collection was derived from nine research participants who agreed to successfully address the business problem by answering ten open-ended questions in a semistructured online, face-to-face interview format. I provided each participant with access to information regarding the business problem and established informed consent. The methodology of online qualitative data collection lends itself to my interpretation of transcripts time and date-stamped transcripts (Wilkerson et al., 2014). Morison et al. (2015) articulated that online interviews are a tool where data collection can freely occur while significantly diminishing researcher input and biases. Wilkerson et al. (2014) noted that a disadvantage of an online data collection method might exist if any participant's ability to gain access to a computer system is adversely affected. Wilkerson et al. further noted that an advantage of an online data collection method is in the creation of an atmosphere of greater openness and expression that may exist due to the observance of anonymity, which applies to the sensitive topic of the analysis of cybersecurity strategies to prevent cybersecurity threats.

The face-to-face interview, administered in an online format, provided anonymity for participant responses. However, the online interview tool may identify the geolocation of every individual respondent. I did not leverage Internet Protocol (IP) search tools or methods to identify respondents' locations following ethical research protocols. The population of small business cybersecurity analysts in this study communicated via email, ensuring that every respondent had access to a computer and the internet. Every research participant was provided with an invitation via email that included an informed consent form. After completing the form, each respondent returned a signed informed consent form stored on an encrypted one drive protecting each participant's identity.

After allocating one week from the email's receipt, which contained the informed consent form, I resent any invitations for the participants to complete the form. I checked for submitted informed consent forms via email from potential participants. I continued the action each week until I obtained the entire set of nine participant confirmations to participate in the study. I then documented the participants' emails that were willing to proceed to the online semistructured interviews of the data collection process. I provided a URL in reply to the informed consent form inserted at the end of the respondents' email, which outlined their willingness to participate in semistructured online, face-to-face interviews where probing questions were asked to detail the ten open-ended questions. Additional questions (see Appendix A) based on participants' responses were presented to gain further insight and clarity on any aspect of the data derived from participants' responses.

Data collection was executed in semistructured interviews in an online, face-to-face setting. Nine participants consented to answer probing questions regarding the ten open-ended questions outlined. Nine participants participated in semistructured interviews in an online face-to-face format to provide additional details from the responses to the ten open-ended questions. Khan (2014) explained that an advantage of the semistructured face-to-face format of data collection offered participants the opportunity to expand upon the intricacies of their strategies and provide greater context around their beliefs. Yin (2013) argued that a disadvantage of the semistructured face-to-face format of data collection, in the form of an online interview, would exist if the questions were formulated or delivered in a biased manner.

The semistructured face-to-face online interview transpired following the time, date, and location as prescribed by each participant to ensure privacy and anonymity (Yin, 2013). Each participant was asked to provide permission and agree to record the face-to-face online meeting during the interview. The recording captured the audio and video of the semistructured online video interview session. Per optimal research practices, I maintained and repeated the same introductory interview process for each semistructured face-to-face online interview (see Appendix B) to curtail bias, as posited by Yin (2013).

The final phase of data collection involved an industry document review, as relevant documents covering current cybersecurity strategies to prevent cybersecurity threats were requested as part of the interview protocol (see Appendix C). Yin (2018) posited that collecting data from various data points provides data collection obtained from several sources necessary when utilizing methodological triangulation. I applied the method by gathering data from relative NIST documents, other related industry-standard documents, and semistructured online face-to-face interviews.

However, before data collection was conducted, I received permission from the IRB. After approval from the IRB, I began to conduct data collection. Participants were provided with informed consent forms with instructions and details regarding the study, which required a signature from each participant before participation in the study could begin. Upon receipt of the informed consent form from each participant, I placed a telephone call or email to engage each participant and provide an introduction to the study. After each participant was briefed on the study, each participant received emails containing instructions for scheduling the interviews. Participants received a scheduled date of their choosing for the online, face-to-face interview and the URL from the Zoom (https://zoom.us) application that facilitated the interview. After the interviews were completed, member checking was executed for the next phase of the study, which provided accuracy for the researcher (Thomas, 2017). Welch et al. (2014) articulated that participants will engage in member checking to validate accuracy, interpretation of their responses, and intended meaning as a form of accuracy assessment. After confirmation of the accuracy of each research participant's responses via member checking, I began to export the study's online face-to-face interview data from Zoom (https://zoom.us), as well as any NIST documentation discussed via participant interviews, and import the data into the NVivo 12 software.

After the interviews were conducted, each semistructured face-to-face interview participant received an email containing a secure electronic password-protected copy of their transcribed interview containing my account of the interview. For member checking, the semistructured face-to-face interview of each of the research participants was reviewed. Each participant performed member checking of their responses provided via an email containing my interpretation of the semistructured online interview transcripts and an online, face-to-face interview. Opportunities for membership checking were provided in the interest of delivering accurate interpretation, correctness, intentional, and exact connotations of the interview (Welch et al., 2014). Once the written confirmation of accuracy was received, after member checking from each participant where no new data was derived, the process of importing the data into NVivo 12 software was conducted.

Data Organization Techniques

The data organization system utilized for this study consisted of research participants' responses to open-ended questions using semistructured online, face-to-face interview responses, relevant NIST documentation, and additional industry-standard publications concerning current cybersecurity prevention strategies. Castillo-Montoya (2016) asserted that the confidentiality and anonymity of research participants are paramount to ethical research. Bengtsson (2016) also noted that ensuring data transparency is another critical aspect of quality research. Shapiro and Oystrick (2018) articulated that using a spreadsheet provides data anonymity and data transparency, making the data readily accessible. I utilized a spreadsheet and NVivo 12 software to codify, organize, and categorize data collections from this study. The spreadsheet is housed on an encrypted OneDrive for security and recovery initiatives. The utilization of a logging system that correlates participant data to indirect identifiers ensures the anonymity and confidentiality of participant names and data (Khan, 2014). All documents regarding each research participant, including my interpretation of the transcripts, industry-standard documentation, recordings, and video, are stored on encrypted password-protected files on a personal OneDrive via access from a PC for five years. In strict adherence to the Walden University research process, data from the research study will be maintained in an encrypted, anonymized, and password-protected format for no less than five years after the study has been completed, upon which after the five years will be promptly destroyed.

Participants who completed the informed consent form confirmed their intention to participate in the study via email. As data was transcribed from interviews and member checking was performed, NVivo helps researchers manage and organize data (Welch et al., 2014). Captured responses regarding the semistructured online, face-to-face interviews were conducted via Zoom (https://zoom.us) recording sessions. Afterward, I provided each respondent with a password-protected file containing a copy of my interpretation of the interview transcript for member checking and written approval, as proposed by Welch et al. (2014). The extraction of the transcriptions occurred after post-member checking from Zoom (https://zoom.us) for import into NVivo 12 software.

NVivo 12 software was utilized to provide qualitative data analysis and leveraged to provide importing and coding functions (Edwards-Jones, 2014). NVivo 12 software provided each transcript, post member checking, with a random number assigned to correlate with each participant's name and a random letter assignment that correlated to each participant's business name as a random letter and number assignment that will maintain the confidentiality of each company and participant.

Following the remote nature of the data collection and interview process, no physical data was stored for this study. All data collected from participants will reside in the same OneDrive folder and within the password-protected NVivo 12 software program. The process solidified access to the data while securing accessibility, protecting security, and ensuring the restoration of the data in the case of accidental deletion. Participants do not have any matching data that would lead to identifying or correlating a research participant's data other than the systems that codified the assigned numbers to protect anonymity. I provided anonymity for research participants by establishing a codified system that linked the letters P1, which translates to Participant One, following a series of numbers ranging from 1 through 9 as participants were coded P1, P2, P3, and P4, and so on leading to the ability to retrieve needed data upon request quickly while providing privacy and security of the data (Nadal et al., 2015). NVivo 12 software inherently provides this function. Upon the end of no less than five years, all data associated with the study will be destroyed following any policies and procedures outlined for the method and environmental safety measures suggested for its destruction.

Notes were cataloged and scanned into a reflective journal to organize any thoughts and themes derived from participants' interviews. Newington and Metcalfe (2014) posited that the utilization of reflective journals allows qualitative researchers to organize their observations, thoughts, perspectives, and points of view as part of the research. Appelbaum et al. (2017) explained that producing a self-reflective research paper promotes reflection to define personal objectives and assumptions and communicate subjective and individual beliefs. I also utilized the reflective journal to identify bias as I documented observations and reflections that could be deemed biased during the data collection process and the possibility that the journal may have added new perspectives to the study.

I provided each research participant of this qualitative pragmatic inquiry with the ability to protect their right to privacy, as posited by Leedy and Ormrod (2015). Research participants' rights to privacy include every measure to protect their company name and identity, as well as any data derived from their semistructured online, face-to-face interviews (Yin, 2013). Electronic scans of all signed informed consent forms, relevant NIST documents, other related industry-standards documentation, transcripts, and recordings received, were stored on the encrypted password-protected OneDrive for no longer than five years from the interview date, with all paper copies immediately shredded after the scanning process.

Data Triangulation

Methodological triangulation may be presented as forms of data that include document reviews, surveys, interviews, and observations, as asserted by Morgan et al.

(2017). Varying themes will emerge during the application of the data analysis phase of the study, methodological triangulation of data sources, and the analysis of data utilizing Yin's five-phase process, as asserted by Yin (2018). Siegner et al. (2018) also posited that when utilizing documents, researchers are provided with greater insight into the subject matter, fostering a greater understanding of the research topic. Yin (2018) further noted that gathering evidence from several sources and converging the data allows for methodological triangulation and analysis of industry documents that help to strengthen the validity of a study. O'Connell et al. (2018) posited that document analysis provides a vehicle for analyzing and reviewing the relevant industry standard documentation relevant to the study. Iivari (2018) also noted that collecting data utilizing several methods and approaches allows the researcher to understand the phenomenon better, cultivating different perspectives while improving validity.

When executing data analysis, scholars posited that employing methodological triangulation adds richness and credibility to the reliability and quality of the research outcomes (Rubin & Rubin, 2012). Renz et al. (2018) noted that methodological triangulation further enhances data quality analysis by providing data verification across multiple sources. Carter et al. (2014) demonstrated that researchers utilize methodological triangulation to assess data validity and reliability by combing data from various sources. Twining et al. (2017) proffered that to enable data triangulation through qualitative research; it requires that data be collected from multiple sources. Renz et al. (2018) posited that methodological triangulation provides a metric to measure and advance data quality via cross-referencing multiple sources of data. Triangulation in the data collection increased the level and veracity of the evidence providing credibility that reinforced the reliability of the data while lowering the risk of bias (Abdalla et al., 2018). Fusch et al. (2015) articulated that triangulation advances iterative themes found within the collected data in support of multiple data collection techniques in a critical analysis of the collected data. I utilized document reviews, online semistructured interviews, methodological triangulation, as well as member checking to provide an adequate level of credibility and validity for the data collection in this study.

Data Analysis Technique

Data analysis provides the interpretation of the tested data (Yin, 2018). Yin (2018) also noted that data analysis allows the researcher to gain a broader meaning of the data that incorporates several factors: preparation, conducting a difference analysis, personal data consumption, and developing an intricate understanding of the data. Leedy and Ormrod (2015) articulated that when researchers emphasize the data collected by leveraging thematic coding to obtain conclusions, qualitative studies consider it a general data analysis practice. Leedy and Ormrod (2015) additionally asserted that when utilizing a pragmatic qualitative research method, the researcher intends to present a complete description of a phenomenon within a specific context in a real-world setting, allowing a liberal amount of flexibility in methods and techniques applied to understanding a not yet understood phenomenon. Bedwell et al. (2015) and Gioia et al. (2012) all articulated that the researcher obtains knowledge and understanding regarding qualitative phenomena by discovering principles, hidden trends, and subjects in data analysis. Thematic coding of the responses can be achieved from the online interview transcripts post-member checking utilizing NVivo 12 software as the basis of a codebook (Ando et al., 2014).

For this study, I utilized the conceptual framework of Cohen and Felson's (1979) RAT as the lens to guide the research study. Cohen and Felson's (1979) RAT is leveraged in this study to explore issues that provide the impetus for cybercrime activities referencing an offender, a suitable target, and the absence of a control or mitigation technique. Exploring participants' experiences of cybercrime as an event may provide insight into variables that propagate a lack of adequate cybersecurity strategies. These variables may also hinder the efficient utilization of mitigation techniques to prevent cybersecurity threats in the small business domain. RAT explained crime as an event that emphasizes its relation to space and time and specifically targets its social and environmental nature and implications (Kigerl, 2012).

For data analysis, I utilized the five-step process as posited by Yin (2018), which examines topics that include data analysis for data collection, decomposing the data, the reassembly of the data, and its interpretation. Yin posited that the process allows for data grouping into themes and topics for better data analysis. It provides a model to take large data composites and narrow them into smaller, more consumable sections of more isolated data. Maguire and Delahunt (2017) noted that grouping data into themes enhances data analysis by creating salient points in the data for review.

I utilized various data collection methods that consisted of semistructured online face-to-face interview responses, NIST documents, and additional industry-standard documentation concerning current cybersecurity prevention strategies to establish a history of documentation to support the employment of methodological triangulation. My data analysis focused on the strategies, policies, and procedures identified within a small business organization to prevent external cybersecurity threats. I reviewed relevant industry standard documentation, interview notes, transcripts, recordings, and other data sources, to glean common themes, topics, and descriptions with each review to achieve data saturation. I reviewed and critically analyzed relevant industry standard documentation to validate the description from the in-depth online interviews. I persisted in the pursuit of identifying major themes from various sources of data utilizing a method of color-coding the data to identify and correlate salient topics and themes. I instituted a repetition system to reveal salient data to inform the research study. I explicitly searched for data that informed my central research question, “What strategies do cybersecurity analysts of small businesses utilize to prevent external cybersecurity threats?” I identified themes and salient points in the data highlighted by various color schemes within the software application NVivo 12 software.

Freitas et al. (2019) asserted that qualitative researchers could utilize software applications to assist in data analysis to elucidate categories, dimensions, and subcategories of analysis. Freitas et al. (2019) further noted that software applications provide an efficient manner of alleviating technical tasks that relate to the organization of the findings that bear no effect on the meaningful outcome of the study and require very little critical analysis. Edwards-Jones (2014) noted that NVivo 12 software is a qualitative data analysis tool utilized by researchers to code data into themes and topics.

I leveraged a software-based data analysis tool called NVivo 12 software for this study. Edwards-Jones (2014) noted that NVivo 12 software does not automatically code the data into topics and themes; however, it does provide a vehicle for the researcher to visualize the data and decide upon the salient points within the common themes. Leedy and Ormrod (2015) further noted that coding themes allow for discovering the correlative experiences of each research participant. The software tool analyzed text-based open-ended questions and transcripts of online interviews post-member checking. NVivo 12 software was critical in providing an efficient coding process for several data sources from the data collected. The data was entered into NVivo 12 software from several data sources utilizing the coding features of the application to aid in the analysis of the data while coding the data into themes, categories, and groups. NVivo 12 software aided in the discovery of relationships as well as any correlations among the composite data. I engaged in specifically elucidating reoccurring themes, correlating topics, and strategies from the multiple data sets during the data collection phase of the study.

Reliability and Validity

Reliability pertains to test results that can be replicated, and validity denotes the accuracy of the data (Yin, 2018). Dikko (2016) articulated that the ability to consistently and without bias accomplish similar outcomes is defined as reliability. Dikko also noted that in a qualitative study, validity would be considered the instrument of measure that has measured the concept of its intended measurement. Forero et al. (2018) purported that confirmability, transferability, credibility, and dependability in a qualitative study are the four criteria for establishing trustworthiness. Twining et al. (2017) further noted that the utilization of analytical processes around these four criteria enhances credibility and trustworthiness in a qualitative study. Titze et al. (2014) asserted that qualitative research seeks confirmability, credibility, and trustworthy findings. Morse (2015) purported that dependability, confirmability, and credibility are replaced by reliability, objectivity, and internal validity in quantitative studies. Yin (2018) also posited that validity engages construct validity, external validity, and internal validity, as reliability and validity are imperative for a qualitative study to validate that the data is accurate and trustworthy. Thomann and Maggetti (2017) noted that rigor could be achieved by establishing qualitative comparative analysis that ensures internal validity, clarifies the question of external validity, and explicitly adopts specific modes of reasoning.

Dependability

Dependability demonstrates repeatable findings as the study is conducted by the same set of research participants, analytical software coding tools, and the same context is provided (Forero et al., 2018). Forero et al. (2018) further noted that ensuring a step-by-step process of documenting the data and a detailed description of study methodologies can also result in dependability within the study. In qualitative research, the researcher can ensure reliable findings by utilizing a very rigid set of interview protocols as well as conducting member checking amongst research participants to validate the accuracy of the interview data (Frels & Onwuegbuzie, 2013; Marshall & Rossman, 2016; Thomas & Magilvy, 2011).

In the execution of this study, I adhered to a rigid set of interview protocols as outlined in Appendix B to achieve dependability as purported by Frels and Onwuegbuzie

(2013); Marshall and Rossman (2016); and Thomas and Magilvy (2011)). I also engaged every participant in member checking to ensure that the data presented, findings, and conclusions were dependable and accurate. I provided a detailed description of the processes followed to collect and analyze the data to ensure the documentation of a step-by-step process that can be replicated to achieve the findings. The attention to detail in data collection, analysis, member checking, and data interpretation provided a methodology to be followed and replicated to enhance dependability (Korstjens & Moser, 2018; Nowell et al., 2017). The strict adherence to research protocols and documented processes provided a window into the logic utilized to reach conclusions derived from the data.

Credibility

Credibility is regarded as the authenticity of the research data from the participants' point of view, as posited by Cope (2014). Validating that the perspectives of the participants are accurate in the study's findings provides research that is deemed reliable and ethical (Cypress, 2017). Researchers utilize member checking to enable participant confirmation that pertains to the correct understanding of participants' responses and the completeness as recorded and interpreted by the researcher (Marshall & Rossman, 2016). Forero et al. (2018) further noted that the researcher achieved credibility by documenting the interview protocol and process and diverse and prolonged engagements with each research participant.

I participated in prolonged engagements with each research participant to ensure ample time to gather the data needed to reach data saturation and conduct member checking until no new data could be derived. I provided rich detail about the interview protocol and process. Korstjens and Moser (2018) touted that methodological triangulation is one of the myriads of critical methods to reach credibility. I utilized methodological triangulation in this study to display and enhance credibility. Korstjens and Moser (2018) further explained that the utilization of member checking in gathering data about conclusions, interpretations, and coded analytical categories would promote credibility. This methodology ensures confidence in the authenticity of responses. I engaged in member checking to validate the accuracy of responses, ensure the study's validity, and provide reliability regarding the content.

Transferability

Transferability instills confidence that the study results can be transferred or generalized across other sets of participants in the context of this study, as noted by Forero et al. (2018). Korstjens and Moser (2018) noted that the reader should determine transferability. They conceptualize whether or not the study applies to their environment or set of circumstances as the emphasis is placed on the reader rather than the researcher to make the determination.

To provide a mode of transferability over which the researchers have no control, I provided thick, rich descriptions of research participants' responses as well as provide clear interpretations of the collected data so that the reader can make an informed determination of applicability across their situation and environment (Nowell et al., 2017). Forero et al. (2018) articulated that transferability is mainly obtained through the critically crucial analytical process of the selection of research participants as well as adhering to methodological triangulation when achieving data saturation where no new data can be derived. In this vein, I documented the process of selecting appropriate research participants for this study and applied thick, rich descriptions of the criteria participants must meet to engage in this study to inform the reader of any functional attributes that they can correlate to their environment across the selection process to promote transferability further.

External validity increases when a set of outcomes can be shared across the population and leveraged beyond a single case study, as noted by Thomann and Maggetti (2017). Thomann and Maggetti further noted that it is imperative to provide a heightened level of care in the participant selection process. Cybersecurity analysts must be screened as participants that can answer the research question. The screening process is key in obtaining a population that possesses the expertise that is feasible, critical, and relevant in responding to the research question. I engaged in a recruiting process that screens the cybersecurity analysts' ability to provide a population that is well-versed in successfully utilizing strategies to prevent cybersecurity threats.

Qualitative studies generalize to a conceptual framework rather than a specific population, as Welch et al. (2014) noted. In generalizing to RAT, this study gained external validity by selecting a population engaged in utilizing strategies to prevent cybersecurity threats to small businesses. The outcomes of this pragmatic qualitative inquiry could be generalized based on RAT.

Confirmability

Confirmability instills confidence that the results are corroborated when other researchers review the findings (Forero et al., 2018). Confidence in the review of the findings is primarily achieved through critical data analysis processes such as methodological triangulation, as posited by Abdalla et al. (2018) and Forero et al. (2018). In alignment with Abdalla et al. and Forero et al., Nowell et al. (2017) asserted that confirmability is obtained through achieving transferability, credibility, and dependability.

To obtain confirmability, I validated that dependability, credibility, and transferability have all been obtained. I utilized and applied methodological triangulation to review, gather, and critically analyze the data while completing this study. I adhered strictly to research protocols and documented processes to provide a window into the logic utilized to reach conclusions derived from the critical analysis of the data. I provided notations of the interview processes that included my interpretations and analytical protocols in the data gathering and data analysis methodologies I engaged in while conducting the study.

Data Saturation

I collected data in the form of semistructured, online face-to-face interview responses, NIST documents, and additional industry-standard documentation concerning current cybersecurity prevention strategies to review the data thoroughly. I also engaged participants in member checking to ensure the validity of my interpretation of the research participants' responses. Ando et al. (2014) pointed out that data saturation occurs when the possibility of eliciting new themes or codes is not achievable from the data collected. In agreement with Ando et al., Mohr and Metcalf (2018) articulated that data saturation is reached when no further data can be derived from the research participants to inform the study. Saunders et al. (2018) further articulated that data saturation involves justifying the amount of data gathered as equal to the data required for research, and no new data can be derived.

Data saturation was achieved by interviewing participants to exhaust all information applicable to the research questions, and no new data was derived. Data saturation was determined by analyzing participants' responses in real-time during the interview while formulating new questions as participants revealed salient points, norms, and constructs regarding the research topic. The purposive sample was sufficient to reach data saturation, where no new data could be derived. It was achieved via interviewing all willing participants within the organizations immersed in the day-to-day operations of preventing external cybersecurity threats.

Transition and Summary

This section of the study emphasized the purpose of the study. It provided information regarding the ethical research aspect of the study, the population, the sample for the study, the research design, and the process for data analysis that aligns with the research design. Also discussed were the researcher's role, methodology, and approaches for data collection. Finally, I described how reliability and validity were addressed. This section provides details of how the study was conducted relative to the conceptual framework and the appropriate data analysis that provide an atmosphere to extrapolate themes and outcomes.

Section 3 includes presenting findings for this study, future research, and themes and subthemes of the composite data. In relation to the research study, social change, personal reflections, and its overall process was elaborated on.

Section 3: Application to Professional Practice and Implications for Change

The focus of this study was to explore the strategies utilized in practice by IT cybersecurity analysts of small businesses to prevent external cybersecurity threats. In Section 3, I present findings from the data collection and analysis to provide a perspective on how the findings may contribute to the academic literature. I also provide a perspective on how the findings may effect social change and professional practice as cybersecurity strategies are being implemented and developed to offer a prospective model for preventing external cybersecurity threats. In closing, I make suggestions for future studies and provided a reflection on the overall study.

Overview of Study

The purpose of this pragmatic qualitative inquiry was to explore the strategies utilized by IT cybersecurity analysts of small businesses to prevent external cybersecurity threats. The data for this study was extracted from semistructured interviews that I conducted with IT cybersecurity analysts in the northern area of Texas. The relevant documents analyzed for this study to promote data triangulation consisted of nine participant interview transcripts, industry-standard documentation regarding the NIST SP 800 series, NIST CSF documentation, ISO 27001, as well as notes derived from participant interviews.

The NIST series includes documentation starting with NIST Framework 800-18 through NIST Framework 800-171, including the NIST Management Framework, which consists of a series of 13 frameworks that features a set of technical standards publications that detail U.S. government procedures, policies, and guidelines on information systems that are developed to address and support the privacy needs of the U.S. Federal Government information and information systems.

Presentation of the Findings

I began this study with the premise of answering the following research question: What strategies do cybersecurity professionals of small businesses use to protect their systems from external cybersecurity threats? In this section, I present the findings from the evaluation of the data I have gathered relating to the research question. The study consisted of nine participants from six organizations with an average of 10.6 years of experience working in cybersecurity, holding a position that provided the protection of PII and assets from external cybersecurity threats. I utilized methodological triangulation in the gathering and reviewing relevant documentation regarding the NIST SP 800 series, NIST CSF, CIS Critical Security Controls, ISO 27001, interview notes derived from participant interviews, as well as transcript data that was scrutinized from semistructured interviews held with each participant via Zoom (https://zoom.us).

The following six major themes were derived from the analysis of the data: (a) applying standards regarding external threats, (b) evaluation of cybersecurity strategies and effectiveness, (c) awareness of the external threat landscape, (d) assessing threat security posture, (e) measuring the ability to address risk and prevent attacks related to external threats, and (e) centralizing communication across departments to provide perspective on threats. I offered an analysis of each of the themes represented in this section (see Table 1).

Table 1

Aggregate of Major Themes for Analyzing Small Business Strategies to Prevent External Cybersecurity Threats

	Interviews		Documents	
Major themes	Count	References	Count	References
Applying standards regarding external threats	9	96	3	32
Consistent evaluation of cybersecurity strategies and effectiveness	9	35	2	37
Consistent awareness of the external threat landscape	9	53	2	26
Assessing threat security posture	9	53	3	21
Measuring the ability to address risk and prevent attacks related to external threats	9	22	2	28
Centralizing communication across departments to provide perspective on threats	9	45	2	24

Theme 1: Applying Standards Regarding External Threats

Cybersecurity analysts cannot properly address the implementation of standards regarding external cybersecurity threats without first understanding the unique position of the organization and what their overall stance is regarding the protection of the organization's PII and its assets. This also entails the prioritization of the assets when applying a risk model that effectively protects each asset, as well as identifying the impact, likelihood, and severity of each external threat. This theme includes four common subthemes: challenges in utilizing industry standards, determining factors for the utilization of industry standards, utilizing NIST as a cybersecurity strategy, and ISO Standard 27001. In the following subsections, I analyze and discuss each finding in relation to each of the subthemes presented (see Table 2).

Table 2

Subthemes for Applying Standards Regarding External Threats

	Interviews		Documents	
Subtheme	Count	References	Count	References
Challenges in utilizing industry standards	9	47	2	9
Determining factors for the utilization of industry standards	7	25	2	9
Utilizing NIST as a cybersecurity strategy	9	17	2	9
Utilizing ISO Standard 27001 as a cybersecurity strategy	3	7	1	5

Subtheme: Challenges in Utilizing Industry Standards

Understanding the organization’s overall business structure regarding its purpose leads to the application of the industry standards was a common theme across all participant interviews. Before cybersecurity analysts can understand the challenges they face when implementing these industry standards, they must be aware of the company’s purpose and how they intend to fulfill that purpose. Understanding business needs is an important theme, as the challenges of selecting and implementing industry standards may differ from organization to organization. Understanding the business needs allows cybersecurity analysts to apply sound cybersecurity policies and procedures coupled with industry standards to adequately protect their organizations from external threats. Each of the participants who were involved in applying policies and procedures discussed the importance of understanding what functions the business carries out to select an adequate industry standard that will be implemented across the organization. The issues concerning challenges regarding the implementation of the industry standards that were discussed included scope, costs, and the ability to have qualified cybersecurity analysts executing the duties of industry-standard implementation, as expressed by Participants 1, 2, 3, 4, 5, 8, and 9. P6 stated, “We have no authorization to provide any input on how the industry standards would be implemented; therefore, we had not experienced any of the challenges when implementing the standards.” P7 indicated that “A good strategy that is widely utilized in the industry is to reach out to other companies to find out how they are implementing these strategies, especially if they were successful at it.”

Support for this theme referencing challenges regarding the implementation of a NIST framework to promote a defense in-depth strategy is not specifically outlined in the NIST documentation and could not be identified within the NIST framework; however, all participants touted that they leveraged NIST to create polices in the prevention of external cybersecurity threats. According to Farber (2018), in a study conducted by the Government Accountability Office (GAO) in 2018, organizations reported four major challenges associated with the implementation of the NIST CSF that included limited resources to commit to implementation, lack of knowledge and skills needed to successfully implement, pre-existing regulatory and other industry-related requirements inhibit implementation, as well as other organizational-related priorities taking precedence over NIST CSF adoption and implementation, which corroborates data extracted from the participant interviews.

Support for this subtheme is validated in the current literature as Selznick and LaMacchia (2018) articulated that small businesses must understand that cybersecurity is regarded as a cost of participating in commerce and a requirement that deserves time and effort when managing. Small businesses are advised to implement strategies that NIST has created, more succinctly frameworks found in the NIST SP 800 series as well as the NIST CSF, formulated in response to the humbling statistics surrounding data compromise that was becoming a sensitive and urgent issue due to its growing prevalence (Almutairi & Riddle, 2018). Mithas et al. (2018) also articulated a global shortfall of about 7 million qualified cybersecurity professionals, which provides the impetus for small and medium-sized businesses to incur a lack of human capital to thoroughly research the broader issues that plague cybersecurity to increase security while lowering costs. Small businesses lack the luxury of dedicated qualified cybersecurity professionals to adequately implement security measures, properly address and mitigate threats, and perform scheduled audits, translating into critical security tasks delegated to workers who lack the expertise to secure the organization, as identified by Berry and Berry (2018). Cybersecurity analysts cannot adequately provide guidance on the implementation of industry standards and its challenges without the required training, addressing shortfalls regarding manpower, as well as knowledge of how the organization intends to conduct business, as posited by all participants.

This subtheme is aligned with this study's conceptual framework of RAT as Cohen and Felson's (1979) RAT is leveraged in this study to explore issues that provide the impetus for cybercrime activities referencing an offender, a suitable target, the absence of a capable guardian, control, or mitigation technique. When these factors are applied to cybercrimes and the ability of a motivated offender to execute a successful breach against a target that lacks a capable defender, we can identify strategies that may prove to be advantageous for small business organizations (Messner et al., 2007). These techniques may lead to directing reinforcements needed as the efficacy of the model was proven to decrease the number of compromised hosts, including after a data breach, as posited by Xiong et al. (2019). Exploring participants' experiences of cybercrime as an event may provide insight into variables that propagate a lack of adequate implementation of industry standards, which may also hinder the efficient application of mitigation techniques to prevent cybersecurity threats in the small business domain. When analyzing the data, the lack of a capable guardian, which applies to the absence of a cybersecurity analyst, an inadequate level of training, or lack of a proper mitigation technique, plays a vital role as the shortfall of about 7 million cybersecurity analysts was noted as a concern when identifying challenges to the implementation of industry standards.

Subtheme: Determining Factors for the Utilization of a Standard

Contextual awareness of the business goals and processes, as well as how they are applied within an organization, are key in determining which standards would best fit the organization. Seven of the nine participants mentioned an understanding of the business goals, processes, and their application as key indicators for the proper determination of utilizing an industry-standard in various forms. For cybersecurity analysts to properly assess the factors when selecting an industry standard, they must understand the business and how to gather data from the various sources as well as how these standards would be applied within a real-world business setting. Participants 1, 2, 3, 4, 7, 8, and 9 each posited that the position they adopted regarding the selection of an industry standard was directly linked to what has been widely utilized within their industry regarding the determination of an industry standard. The standard, which was correlated to how that business functions, is usually the industry standard that has been deemed effective in the protection of various organizations. The protocol that is leveraged in the determination of an industry standard, as noted by Participants 1, 2, 3, 4, 7, 8, and 9 has data that suggest that this has not been an effective process as data breaches have become so widespread that it is now seen as a part of the process of engaging in commerce as threats are ever-changing and evolving (U.S. Department of Commerce, 2017). P5 stated that "when selecting a standard, it is in direct relation to what has usually been adopted by our counterparts." P6 articulated that "C-level executives are highly concerned about the budget and that all ideas must be shared with senior management before a consensus can take place." They explained that they have very little authority in making business-altering changes or recommendations regarding the utilization of standards as the final decision remains with the C-level executives. P5 and P6 indicated that the utilization of the standard, when selected maintained a certain level of confidence amongst C-level executives that consisted of assurances of security when facing external threats. Participants 1, 2, 3, 4, 7, and 8 indicated that the industry standards are usually determined by what is deemed effective within their industry. Leveraging data that have been shared across an industry provides a baseline of standards that can glean expected results. P1 articulated that at some point, innovation and new technologies must play a role in the determining factors regarding providing many levels of defense along with the industry standards, no matter the costs.

Support for this theme is not directly addressed and is considered widely subjective when addressing the factors for the determination of the utilization of a standard. All of the participants leveraged an NIST framework and utilized the standards to help create policies to secure their systems. However, there are no references found in the NIST documentation to corroborate how and when the utilization of the standard should be applied within an organization. However, in the NIST CSF, which was not specifically referenced by participants of this study, the application of this voluntary framework provides guidance as to its efficacy, touting that it helps businesses of all sizes to better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The NIST CSF provides businesses with an outline of best practices to help decide where to focus their time and money regarding cybersecurity protection (Federal Trade Commission [FTC], 2022).

This theme is supported in the literature. For a small business to meet compliance, cybersecurity analysts must relay concerns and cybersecurity needs while remaining consistent in utilizing systems that ensure its infrastructure's confidentiality, integrity, and availability (Kakucha & Buya, 2018). A small business is tasked with overcoming many obstacles when trying to maintain viability and create a culture that promotes safe cybersecurity practices, as the employees must possess the ability to adapt to a changing and diverse environment where efficiency in management, leadership, as well as understanding the strengths and weaknesses of the organization's risk tolerance are keys to survival (Schoemaker et al., 2018). As small businesses obtain state-of-the-art technologies, there are additional risks to the organization and its data transfer methods, including cloud computing, 5G technologies, and introducing IoT into the network (Au et al., 2018). The apparent issue for small businesses is the cost of the technologies and the cost of implementation and training for these new forms of data communication that pronounce new and improved confidentiality, availability, and integrity measures (Berry & Berry, 2018). As technologies are integrated into the small business and avenues for more significant revenue streams, and efficient allocation of resources are created, small business leaders must be knowledgeable about the pitfalls that may affect their bottom line and compliance (Calvard & Jeske, 2018; Hintze, 2018).

When applying the conceptual framework of RAT, one of the central tenets of the framework consists of exploring issues that provide the impetus for cybercrime activities referencing an offender, a suitable target, and the absence of a control or mitigation technique, as posited by Cohen and Felson (1979). Delays in selecting the correct industry standard will correlate to the lack of a capable guardian or mitigation technique if the understanding of the variables of the business functions, processes, and their application are not presented in a timely manner. Exploring participants' experiences of cybercrime as an event may provide insight into variables that propagate a lack of adequate application of cybersecurity strategies, which may also hinder the efficient usage of mitigation techniques to prevent cybersecurity threats in the small business domain. When these factors are applied to cybercrimes and the ability of a motivated offender to execute a successful breach against a target that lacks a capable defender, which consists of adequately understanding business processes that allow a timely selection of effective industry standards, we can identify strategies that may prove to be advantageous for small business organizations (Messner et al., 2007).

Subtheme: Utilizing NIST as a Cybersecurity Strategy

The utilization of NIST was a reoccurring theme amongst all nine participants as they touted its successes and its broad application. P3 stated that "We utilize NIST because it is the American standard, is well known, and the most utilized in the industry." In contrast to the subtheme determining factors of the utilization of standards, participants were more focused on the broad application of NIST and the perception of its success in the industry despite the data that contradicts its perceived success amongst small businesses. By evaluating data sources that provide insight into where the vulnerabilities exist and applying controls to adequately reenforce those systems, cybersecurity analysts can provide a better application of resources for small businesses. Developing skills that would help to create a partnership between the C-level executives and the analysts would provide a level of trust that can be leveraged to make better decisions when creating strategies to prevent external threats. P9 stated,

> We basically have what we call the cloud security posture management platform that traverses different industry standards such as NIST, ISO 27000, and Azure Security Benchmark that looks across different industry standards to identify if we are complaint with those standards. The challenge is more the remediation process which means there are so may resources and different workload owners that it becomes a challenge to be up to date with everything as there are new vulnerabilities being discovered on a daily basis.

P4, when asked about utilizing NIST as a strategy, regarded that the people, processes, and technology are the concerns when applying such a strategy. Out of those roles, when implementing NIST, people, and processes pose the most significant concerns. P4 stated, “We can get the bodies in, but they are not being utilized or inexperienced and not used to working with technology. There is a ramp-up period where we will experience a lot of inefficiencies.” P4 also indicated that they preferred ISO, but NIST is the American answer when utilizing an industry standard. The more globally accepted explanation is the ISO standard, which covers several security controls.

All nine participants indicated that NIST is the most recognized standard and provides a comprehensive approach to lowering risks. A critical strategy involving greater communication with C-level executives and more leverage in providing authority to define a strategy would prove advantageous when allocating resources to small businesses.

NIST frameworks that align with this theme are an integral part of any approach that contributes to implementing policies within an organization utilized by participants that include NIST Frameworks 800-30, 800-39, 800-82, 800-161, NIST CSF, as well as the NIST Management Framework. Gordon et al. (2020) opined that NIST CSF is an approach that is broadly accepted that facilities cybersecurity risk management within an organization. This sentiment establishes a consensus with the participants interviewed for this study. NIST frameworks have been instrumental in the creation and implementation of organizational policies on several levels aligning with documentation cited by participants of this study referencing the NIST SP 800 series.

When perusing the literature to substantiate the subtheme, I found indications that cybersecurity resource allocation in small businesses is a delicate balance between the C-level executives, which their buy-in is a significant factor in approving cybersecurity initiatives, and its perception as some view its function as a cost rather than a needed investment that protects their organization from company ending data breaches and liabilities (Raghavan et al., 2017). Karanja (2017) noted that uncompromising leadership usually consists of C-level executives who have experience making company decisions during a crisis and provide critical insights into security and governance procedures. The role of cybersecurity, C-level buy-in, management, and its implementation within a small business must be shared by all, from the unheralded cybersecurity analyst to the chief information security officer of the organization (Rothrock et al., 2018).

When comparing the basic concepts of RAT, the absence of a capable guardian is key. When the flow of information is not allowed, the guardian is less effective in providing a strategy when examining external cybersecurity threats. The lack of a capable guardian translates into the fact that the flow of information between the cybersecurity analysts and the C-level executives renders the analysts less effective. Cohen and Felson's (1979) RAT is leveraged in this study to explore issues that provide the impetus for cybercrime activities referencing an offender, a suitable target, and the absence of a control or mitigation technique. When reviewing the research, the researcher's goal was to provide data that would measure the effectiveness of a more capable guardian's effectiveness while reducing the targets' suitability to prevent, intervene, and respond to incidents (Choi et al., 2018). When viewing the IT problem through the lens of RAT, it would prove logical to understand the areas we can better affect positive change through the creation of compensating controls, which would be the element of the capable guardian and the suitable target being the IT cybersecurity analyst and the small business respectively (Messner et al., 2007). Providing a conduit by which the C-level executives and the cybersecurity analysts can provide greater dialogue concerning the application of security controls provides a measure that seeks to increase the guardian's capability to remove ambiguity when choosing an industry standard.

Subtheme: Utilizing ISO Standard 27001 as a Cybersecurity Strategy

When discussing strategies, some organizations find alternative standards to be a better fit, considering their business goals, other than the highly touted NIST amongst the nine participants. Three of the participants discussed the importance of ISO Standard 27001 as a better fit for their organization. P4 stated,

> In our organization, we use an amalgamation of standards. We utilize NIST when it is needed as it provides a blanket strategy when checking boxes for audits. … We also leverage CIS Critical Security Controls that consist of 18 security controls that are effective for cyber defense that runs from inventory and control of assets to data protection…We are not opposed to grabbing controls and standards to build a wall of security for our organization. … Out of all the standards and controls, my choice would be the international standard ISO 27001.

P6 provided a similar perspective when discussing the ISO standard, as they regarded ISO as being very adept at preparing organizations to implement other standards. P8 stated that "ISO provided very little to no roadblocks when implementing the standards."

Participants P4, P6, and P8 stated that ISO was a better standard if you want to provide comprehensive security when meeting compliance with audits. P4 stated, “The ISO standards cover quite a bit, even amongst the global community, and ISO is a better fit for our organization.” P6 added, “When I was an auditor, ISO was very good at preparing an organization to meet compliances and lay the groundwork for other standards.” P8 similarly stated,

> When looking at inefficiencies that would be noticeable for the standard, I really can’t say that any were found as it is a pretty comprehensive standard, and when it was time for implementation, no one would give us a hard time.

These participants were in consensus that the ISO Standard 27001 provided a more comprehensive way of covering the areas that met compliances within their organizations. The participants noted that depending on their business vertical, regulatory, and legal aspects of the business, the ISO standard provided an option that allowed for a process to assess the business goals that would lead them to select ISO over NIST. NIST is seen amongst professionals as a template to follow when you are in the process of creating policies and procedures for your organization, as ISO is for the more mature security application when seeking certification.

The literature resonates with the idea that one of several key attributes of cybersecurity analysts is to provide sound cybersecurity strategies when protecting organizations from external threats. The literature provides studies that are congruent to this theme, as many studies have heralded the cause of selecting cybersecurity analysts that can provide strategies that are effective in preventing data breaches, particularly from external threats. Thomann and Maggetti (2017) noted that it is imperative to provide a heightened level of care in the participant selection process. Cybersecurity analysts must be screened as knowledgeable participants that can make sound decisions when protecting organizations form external cybersecurity threats. The screening process is key in obtaining a population that possesses the expertise that is feasible, critical, and relevant in providing recommendations for strategies to be vetted by each organization. Harris and Patten (2014) indicated that larger businesses and corporations are empowered with adequate resources to recruit, train, and implement diverse and experienced cybersecurity analysts, unlike their smaller counterparts. When obtaining cybersecurity analysts, the unsuspecting user remains one of the weakest links in the cybersecurity network, as posited by Budzak (2016). McDermott et al. (2019) pointed out that the effectiveness of APTs is directly related to the ability of this method of attack to go undetected while showing no signs of infection and evading even experienced cybersecurity analysts.

When aligning to the concepts of RAT, the occurrences in time and space where a motivated offender meets a suitable target due to the lack of a capable guardian is a key concept of RAT and usually results in a physical crime being committed (Cohen & Felson, 1979). Some researchers state that the same occurrence can also be translated into a virtual environment; in contrast, Kulig et al. (2019) indicated that the original concept of RAT did not provide an adequate definition of the attributes of a motivated offender, as Cohen and Felson conceded this limitation and indicated future research was needed to understand offenders' motivation for the crime. However, Reyns et al. (2011) noted that the application of the network-based crime triangle displays how RAT can be expanded to include crimes with distance as a factor in which motivated offenders and suitable targets do not intersect at a physical location. In cybercrime, as the motivated offender and the suitable target exist within the same network, the distance between these elements is not as exaggerated as one would think. Studies, where researchers have specifically utilized the systems approach, have indicated that the concept of RAT can be successfully extended to cyber-related crimes (Reyns & Henson, 2015). The virtual environment links time and space between the motivated offender and the suitable target. The capable guardian plays a significant role in this intersection of time and space; as the guardian's capability is increased or decreased, it may affect the offender's motivations. Cybersecurity analysts who possess the knowledge to properly assess the strategies that are effective in the prevention of external cybersecurity threats would provide an increase in the capability of the guardian that would affect the defenders' motivations, translating to added protection for each organization against external cybersecurity threats.

Theme 2: Evaluation of Cybersecurity Strategies and Effectiveness

Continuous evaluation of cybersecurity strategies and their effectiveness are imperative to an organization to provide preventive measures and controls that are relevant in thwarting current external threats. Cybersecurity analysts play a major role in protecting the PII and the intellectual property that is housed within an organization's networks. The emergence of new threats and technologies that provide increased processing power in the hands of less skilled offenders narrows the gap between organized attackers and the script kiddies seeking to breach private networks. Small businesses are now seeking to provide quality training and personnel to effectively prevent breaches from new external threats existing outside their networks. This theme consists of four subthemes: identity and access management, cloud security, innovation as a strategy, and automation (see Table 3).

Table 3

Subthemes for Consistent Evaluation of Cybersecurity Strategies and Effectiveness

	Interviews		Documents	
Subtheme	Count	References	Count	References
Identity and access management	4	4	2	9
Cloud security	3	9	2	6
Innovation as a strategy	7	11	4	9
Automation	3	11	3	13

Subtheme: Identity and Access Management

Providing a comprehensive cyber security strategy was a common theme discussed by various participants. The forefront of protecting systems from external threats begins with identity and access management. Participants were highly engaged when discussing strategies consisting of a host of the latest tools and technologies that ensure systems are being protected by limiting access to the instance where the systems could be compromised. The utilization of several levels of security is a concept outlined for providing a very robust cybersecurity plan known as “defense in depth” amongst the cybersecurity community. Participants were in agreeance that the tools and technologies utilized to ensure the organizations are protected are only as good as the cybersecurity analysts who are adequately trained on how to correctly apply the technologies to mitigate user error or misconfigurations.

Eight of the nine participants provided insight on some form of mitigating strategy in their responses if systems happened to be compromised. When discussing the various forms of access management, P4 touted that "Should an attacker gain access to the system, make sure that they don't have authentication to be able to go anywhere else." P5 identified various numbers of companies that were being evaluated for third-party identity and access management features and considered the move money well spent for their small business. P7 articulated regrading identity and access management that "if an effective deterrent is in place, it doesn't have to be a century or a guardian because if you can't gain access through your badge or some type of identity mechanism, you're not going to get access." P9 posited that identity and access management is one of the main concerns because a lot of attacks are basically seeking to compromise the identity to gain access to the system. All the participants mentioned that protecting the systems through identity and access management systems is an effective way to provide another level of security within a network while implementing various levels of security controls.

In accordance with this theme, the NIST documentation reviewed corroborates the information derived from participant interviews. Identity and access management has a responsibility to publish and maintain a roadmap for the development of new and to update existing guidance related to Identity and Access Management (ICAM) as it presents milestone activities, projected activity completion dates by fiscal year quarter, and exploratory notes regarding NIST 800-63A series.

As identified in the literature, small businesses provide a conduit through which cybercriminals have access to larger corporations' supply chains within the 16 critical infrastructure sectors. If breached, they pose a considerable threat to national security (Department of Homeland Security, 2019). Identity and access management becomes even more critical in these situations where smaller organizations can affect the security posture of larger organizations. As Von Solms and Von Solms (2018) articulated, the meaning of the term cybersecurity translates to protecting data from unauthorized access or attacks fitted for exploitation. In the first six months of 2019, 4.1 billion records and health-related data were compromised. Some of the most significant data breaches were perpetrated on AccuDoc Solutions and Equifax with third-party relationships with small businesses (Internet Crime Complaint Center, 2018a). Without the proper application and efficient utilization of cybersecurity strategies to protect personally identifiable customer information, society is vulnerable to the unauthorized access and illegal usage of personally identifiable customer data housed by small businesses (NIST, 2019a).

As noted in the concepts of RAT, Cohen and Felson established the RAT in 1979 to explain crime as an event. Essential concepts within the framework of RAT consist of the absence of a capable guardian, a motivated offender, and a suitable target (Kigerl, 2012). Identity and access management affect the concept two-fold by creating another layer of defense that is less desirable for an attacker; ergo, creating a less suitable target as well as increasing the capability of the guardian by adding another layer of defense. Reyns et al. (2011) argued that a networked system could be the space for the interaction consisting of the target and the offender as a substitute for the physical environment.

Closing the gap between cybercrime and physical crime may provide cybersecurity analysts with the data policymakers require to enact laws needed to curb cybercrime. This data can provide cybersecurity analysts with a model that centers the focus on the target creating an atmosphere in the control of the small business. Wen-qun (2006) also asserted that the divide exists between technologies used to execute cybercrime and real-world physical crimes, which lends itself to difficulty in adequately mitigating cybercrime; however, Griffioen et al. (2021) proposed that the connection is made between the divide between cybercrime and physical crime, as well as innovative internal applications that can be framed based on these factors leading to positive change that efficiently mitigates cybercrime by adding greater obscurity to a system hindering the external attacker's ability to gain knowledge within a network as identity and access management could prove to be affective in this context.

Subtheme: Cloud Security

The emergence of new data-driven proprietary applications allows cloud security to play a significant role in how small businesses can protect their systems, equipping some organizations with the ability to garner third-party resources to better protect their assets, as with newer technologies comes a range of varying costs. Cybersecurity analysts were all on board when it came to applying new technologies as this helps provide "one pane of glass" to view many aspects of cybersecurity in one centralized view. In one instance, as indicated by P6, new and innovative cloud-based strategies that mitigate vulnerabilities and protect against evolving threats can be beneficial in aiding small businesses in dealing with these costs (Liang et al., 2018). However, some cybersecurity analysts are cautious when implementing these technologies as eight of nine participants were in agreeance when recommending leveraging cloud security systems; however, P9 stated that "It is complicated because what happens when we leverage the cloud environments everything is connected to the network from external sources, so this leads to even more entry points on the network." All participants were in agreeance that all of their organizations leverage some form of a cloud security apparatus to effectively monitor and protect their systems from external threats. P1 and P5 indicated that the innovation of cloud security, with its ability to provide many options, increases its efficiency when protecting against external threats. P9 stated,

> I think that cloud security has leveled the playing field when competing with larger organizations allowing us to provide next-level security when protecting against external threats; however, … I feel a skills gap exists, and the ability to obtain those individuals that have the knowledge to properly utilize the technologies becomes increasingly difficult as our organizations cannot compete with the salaries of larger organizations.

P1, P5, P8, and P9 discussed their satisfaction with the way the cloud technologies are leveraged within their organizations and plan to provide recommendations for an even greater presence of cloud security technologies in the short-term future, as all expressed that they were firmly in favor of seeking new technologies within this platform to provide even greater data protection. P5 indicated,

> We utilize AWS (Amazon Web Services) as a provider upon which they invoke multiple levels of security. This service provides a collector within the client's

environment that can be utilized on-prem as well as a cloud data collector for the examination of not only data but also for alerting and policies.

The NIST documents reviewed provide support for the participants' approach to this theme as participants expressed their opinions that aligned with the information from NIST documents cited during participants' interviews. A salient point that surfaced in the documentation relayed that NIST Special Publication 800-144 provides an overview of the security and privacy challenges facing public cloud computing and presents recommendations that organizations should consider when outsourcing data. This addresses issues regarding the concerns cited by P9 that referenced the complexity regarding the protection of several entry points due to their connection to external sources when leveraging a cloud environment.

As advanced in the literature, one of the key responsibilities of security analysts is the ability to identify threats and garner the applications necessary to adequately address each threat. This would also include assessing the risk and providing an analysis to determine if the control exceeds the amount of risk perceived. This is further confirmed by the literature as Au et al. (2018) noted that small business seeks to employ various forms of technology to compete with their larger counterparts while providing an acceptable level of due care in protecting customer-sensitive data by leveraging encryption technologies as well as newer technologies that includes cloud-based platforms. Berry and Berry (2018) articulated that in contrast to the amount of costs of a breach per incident that recovery costs are considered significant to small business owners reporting that the average cost of an incident routinely resulted in a cost of

$20,000 per incident and as high as $44,000 in direct costs to the organization which assures small businesses that the investment in the newer cloud technologies is a sound business decision. To compete with the skills gap Bell (2017) articulated that cooperation that relies on the sharing of information between private and government sectors will be needed to form initiatives that will aid in the prevention and mitigation of cyberattacks.

RAT, as established by Cohen and Felson (1979), was used to explain crime as an event that consists of key concepts that are hinged on the motivation of the offender, the lack of a capable guardian, and the inference of a motivated offender regarding the deterrence of a physical crime. Hawley (1944) touted that increasing the capability of the guardian while making the target less suitable contributes to the frequency of crime rates allowing cybersecurity analysts to provide strategies that would positively affect data breach rates in theory. Griffioen et al. (2021) proposed that the connection is made between the divide that consists of virtual cybercrime and physical crime; this would also include the innovative internal applications that can be affected based on these factors leading to positive change that efficiently mitigates cybercrime by adding greater obscurity to a system and the utilization of more effective technologies while hindering the external attacker's ability to gain knowledge within a network. Cybersecurity analysts can provide greater protection for their organizations when merging the concepts of MTD, providing an adequate selection of new technologies, and the utilization of the practical concepts of RAT.

Subtheme: Innovation as a Strategy

Strategically providing avenues to new technologies such as UBA (User Behavioral Analytics), machine learning, and shared communications across businesses were common themes that were raised among the various participants. However, this theme is quite nebulous as its processes for the implementation of the technologies do not follow a standard across each organization. Therefore, the selection for each of the technologies is narrowly based on the need. It is more loosely based on the data, or lack thereof, as well as the personnel that are decision-makers within each organization. Organizations appear to be gathering data to better select technologies for their future cybersecurity needs. Their future cybersecurity needs consist of building a knowledge base around threats and the threat landscape. These strategies were stated as being closely related to where cybersecurity analysts are in their understanding of the new technology. This simply indicates that most technologies are being selected as it pertains to the cybersecurity analysts' level of training associated with the new technology. This theme is related to how innovation is leveraged and whether there are protocols in place that provide a path to ensure that effective technologies are being selected to better meet each organization's cybersecurity needs.

Seven participants opined some form of strategy to ensure that their organization is seeking more effective technologies in preventing cybersecurity threats. When explaining how they select from a host of various technologies and services to foster innovations that are cost-effective to help prevent cybersecurity threats, P1 explained that ”we thought it better to build a knowledge base around whereby understanding is centralized around the threat and the threat landscape." P2 stated that: "We have two new employees that are being trained as well as our groups are being redistributed once again into different groups." P4 articulated that innovation within their organization is stagnant due to the lack of hiring senior engineers, senior developers, and an incident response group. These departments will not be able to provide efficient processes or proper documentation due to the lack of experience. P5 instituted a new mode of communication and workflows that provided partner organizations with information regarding new threats and/or specific events that, if discovered by them or their partner organization, they would share the information across organizations to better prepare them for the coming threats. P6 provided an approach that fostered innovation regarding the simplifying or merging of processes that can be adjusted to their referenced framework. P7 stated the utilization of vulnerability scanning technologies and identifying identity-type tools against probing were most effective. They were to be used in conjunction with organizational frameworks to understand the "different tactics and techniques from all the different players." P9 stated that "we utilize a lot of tools that leverage machine learning so as to learn more about user behavior to understand, for example, patterns of access." All the participants recognized the importance of providing new ways of detecting threats while keeping costs manageable in an attempt to compete with their larger counterparts. Participant methods are diverse; however, each participant was engaged in varying levels of threat detection and data protection as the end goal for the implementation of innovative technologies.

NIST documentation does not exclusively outline innovation as a defense-in-depth strategy in support of this theme; however, innovation is an integral part of providing cybersecurity for a small business as well as providing cost-effective avenues which allow small businesses to compete with their larger counterparts in protecting their organizations.

As validated in the literature, determining factors in fostering innovation consist of managed growth, technology, and innovation while assessing escalating risks, implementing state-of-the-art cybersecurity technologies, and assessing the threat landscape (Martin et al., 2017). Due to the myriad of innovations provided that protect small businesses from external cybersecurity threats, organizations should be aware of the financial constraints when selecting the technological innovations that best fit their organization's budget. The limited resources of each of the organizations do not allow for much innovation or analysis of cybersecurity incidents (Almeida et al., 2018). Small businesses must make applicable data-driven decisions and create standards that provide a picture of what is needed to better prevent external cybersecurity threats when applying budgetary constraints. Small businesses do not possess the budgets of their larger counterparts, as this plays a role in the quality, amount of staffing, training, and technology when implementing their cybersecurity strategy (Kobe & Schwinn, 2018).

When applying the concept of RAT, it defines three aspects of a crime that is needed for the crime to take place. This consists of essential concepts within the framework of RAT that involve the absence of a capable guardian, a motivated offender, and a suitable target (Kigerl, 2012). These are seldom utilized concepts within small business innovation strategies framework. Henson et al. (2016) noted that physical interaction within a specific time frame might not be a mitigating factor when leveraging RAT in cyberspaces if the target and the offender eventually converge; however, these techniques may lead to directing reinforcements were needed as the efficacy of the model was proven to decrease the number of compromised hosts, including after a data breach, as posited by Xiong et al. (2019). Cybersecurity analysts are better prepared to enact change that they can directly control is that of altering the condition of the capable guardian and how its capabilities can be tuned indirectly by providing an adequate pathway or protocol to follow that is standardized, which allows cybersecurity analysts to utilize data and their threat landscape to provide actionable innovative techniques.

Subtheme: Automation

The utilization of automation within the processes of cybersecurity adds significant value and efficiency to external threat prevention strategies. Because of the costs that are incurred by utilizing tools and technologies to better protect small businesses, automation is a strategy that can help to level the playing field when properly utilized. Technologies such as intrusion detection systems and its methods have been utilized to prevent common threats by leveraging a form of automation based on a set of rules; however, the cost of providing these technologies, implementing the solutions, and maintaining these processes are of concern to small businesses (D’Arcy & Lowry, 2019). With increasing costs of the technologies used to prevent external cybersecurity threats and the manpower needed to assess and mitigate these threats, the need for automation becomes clear.

Seven of nine participants mentioned the utilization of automation to help in the detection, prevention, and tuning of systems associated with the mitigation of external cybersecurity threats. P1 noted that they leverage automation and have been very successful at its implementation and provided positive insights for its future within their organization. P2 indicated that "basically what we are trying to do is to …find anywhere we can automate." P3 and P4 indicated that they rely heavily on automation for a significant amount of their eternal threat prevention as it is mostly handled via automation. P7 noted that "budget is a key driver in whether we can purchase certain technologies, and automation helps to alleviate some of those costs so they can focus on the real threats." Relevant industry-standard documentation analyzed further enforced the concepts of automation as a vital part of the iterative process in the prevention and detection of external cybersecurity threats discussing the need for systems that ingest machine learning to better protect their systems, such as leveraging Splunk to support the NIST CSF (Cybersecurity Framework). P3 indicated that "most of our prevention capabilities are automated… as we are trying to think of new ways... we are ultimately trying to tune up current rules so they can provide better automation so that we can keep our eyes focused on real threats." Without the implementation of automation within a cybersecurity strategy, it would be an arduous task to handle each technological capability from a human-resourced perspective (Sravanthi & Nisha, 2021). With the exceedingly large volume of external threats and the systems that analyze the veracity of those threats, it would be impossible to assure the validity of those systems. The efficiency of the system would be highly degraded and not of any real use to cybersecurity analysts.

NIST documentation does not exclusively outline automation as a defense-in-depth strategy in support of this theme; however, automation is required to provide a level of efficiency that allows cybersecurity analysts to then focus on the critical security threats to valuable assets while leaving the "lowering hanging fruit" for automation services to mitigate as in accordance with data retrieved from participant interviews.

When reviewing the literature, automation is key in the prevention of external cybersecurity threats and is now opening up doors for the next evolution in the prevention of external cybersecurity threats hinged on AI (Artificial Intelligence) (Lino et al., 2019). Automation is key in alleviating the noise that is found associated with the detection of threats, and AI has promising applications that are gaining in notoriety and impact securing systems positively; however, more research is needed to analyze the social and ethical concerns of applying the technology (Grosz & Stone, 2018). Automation of technology is a required aspect when mitigating external cybersecurity threats as they are growing exponentially, and it is not feasible to work with traditional models leveraging human intelligence (Sravanthi & Nisha, 2021).

When identifying one of the key aspects of RAT, it is to increase the capabilities of the guardian to provide an improved outward-facing attribute of security while becoming a less suitable target when in the sights of an attacker (Choi et al., 2018). This is accomplished by utilizing automation as a strategy. Maluf et al. (2018) posited that an attack could still occur in an environment with adequate cybersecurity when a motivated offender seeks to find a suitable target to stage an attack. Hawley (1944) touted that increasing the capability of the guardian while making the target less suitable contributes to the frequency of crime rates allowing cybersecurity analysts to provide strategies that would positively affect data breach rates in theory. The overall goal is to become a less suitable target by shoring up defenses and implementing automation which is a key element of this concept (Sravanthi & Nisha, 2021). When reviewing the research, one of the researcher's goals was to analyze data that would assess the plausibility of a more capable guardian while reducing the suitability of the targets to prevent, intervene, and respond to incidents (Choi et al., 2018). An effective way of increasing the capability of the guardian is the implementation of automation, which is not only key in this aspect but in all aspects of cybersecurity. Potentially we want to provide more innovative strategies where the efficacy of the capable guardian is not diminished (Young & Yung, 2017).

Theme 3: Consistent Awareness of the External Threat Landscape

The ability to formulate comprehensive policies and procedures that investigates the threat landscape and identifies threats that are relevant to the organization requires informed threat intelligence, and analysis from various sources are critical strategies needed to properly prepare and respond to ever-evolving threats. In the absence of informed threat intelligence and analysis from various sources for threat identification, a cybersecurity analyst cannot properly provide strategies to mitigate external threats based on the current threat landscape. The inability to provide an accurate landscape of threats that are pertaining to the organization can invariably lead to an inordinate number of unidentifiable attacks leading to a higher instance of data breaches (Gwebu et al., 2018).

This theme consists of three subthemes: most prevalent attacks, vulnerabilities, and threat motivation deterrence as a practice (see Table 4).

Table 4

Subthemes for Consistent Awareness of the External Threat Landscape

	Interviews		Documents	
Subtheme	Count	References	Count	References
Most prevalent attacks	8	24	2	9
Vulnerabilities	6	11	4	10
Threat motivation deterrence as a practice	6	18	3	7

Subtheme: Most Prevalent Attacks

Some of the most prevalent attacks that were discussed from the standpoint of cybersecurity analysts revolved around the threat of social engineering. Small businesses must understand the threat that involves more of a human factor than a technological one. The goal of the attacker is to bypass the technological controls that organizations spend the lion’s share of their budgets on in hopes that they can entice the user into clicking on a link, thereby; bypassing the controls that have been established to prevent external attempts of data compromise and privilege escalation. When asked about which attacks appear the most often within their organizations, eight of the nine participants believed that phishing emails were the most common threat within their organization. Additionally, relevant NIST documentation and other sources that were analyzed that met industry standards referenced security and awareness training as an important aspect of an overall security strategy. Every organization was involved in security and awareness training and saw the threat as one that should be addressed at varying levels of the organization, beginning with all employees and a reporting structure. P1, from an organizational standpoint, regarded the most prevalent threats as authentication or brute force attacks that reside at the layer three and layer four levels, which may include mac spoofing and asset-based attacks. P2 and P3 also articulated, besides the aspect of phishing, which can be easily perpetrated by sending thousands of emails in one campaign with little or no effort, as a huge issue that recon was another attack that was prevalent due to their organization being scanned multiple times a day. P5 discussed, besides the apparent phishing concerns, that drive-by downloads were another issue that raised grave concerns within their organization. “The drive-by downloads turned out to be huge…as being on the cyber defense team, we discovered that various personnel were actually downloading applications that were malicious.” P6 articulated that social engineering was the most prevalent attack via phishing emails, but they were also exposed to ransomware, patch vulnerabilities, as well as distributed denial of service attacks that were being exploited. P7, P8, and P9 agreed that the most prevalent attacks that were being addressed were phishing with some variant of cross-site scripting and IP probing.

The NIST documentation analyzed supported this theme as the most prevalent attacks were found to be social engineering-related attacks. The participants expounded on their opinions regarding this theme as their approach corroborated information gleaned from NIST documentation to combat, prevent, and provide controls to help mitigate the damage associated with social engineering attacks. Wiley et al. (2020) touted that to comprehensively combat social engineering, organizations should commit their focus to the security culture to save time as well as resources while improving security and awareness, which depends on the resolve of organizational leaders to encourage positive security behaviors endorsing transparent decision-making processes, communication, and strategic management. NIST Framework 800-30, 800-39, 800-82, 800-161, as well as the NIST Management Framework that provides details regarding training, best practices, as well as a risk management framework to establish and sustain a secure cyber environment.

When understanding the literature, many researchers articulated that organizations provided some level of training and some sort of user behavioral analysis system that would alert cybersecurity analysts when a malicious link was executed. Fellnhofer (2018) proposed that security and awareness training would be a helpful tool for business leaders to provide an option that would reduce the attack footprint creating a more secure network environment. As a deterrent and correction of the unwanted behavior, it is also achieved through a rigorous system of testing that alerts an organization when an employee clicks on an email from a suspected external threat and has utilized malicious social engineering techniques to enter the network without authorization (Prajogo et al., 2018). Based on participants' interviews, social engineering appeared to be the biggest threat within their organizations and has been the direct causation of many data breaches to this date. These findings tend to mimic the top cybersecurity threats to small businesses, where they incur the most significant financial hardships, consisting of threats that include phishing or social engineering, ransomware, web-based attacks, malware, stolen devices, and denial of service attacks respectively (Ponemon Institute, 2018).

Wolverton and Stevens (2019) acknowledged that some studies demonstrate security and awareness training as effective methods in mitigating susceptibility to phishing attacks; however, other studies have shown that even after completion of the employee-sponsored security and awareness training, one-quarter of the participants were just as susceptible to the phishing attacks. The implementation of several iterations of training and a reporting structure appears to be the best approach going forward to mitigate the success rates of phishing campaigns.

When analyzing the concepts of RAT, social engineering being accepted as the most prevalent attack amongst cybersecurity analysts that reside at the organizations from this study is not specifically addressed in RAT. However, the concepts of improving the condition of the lack of a capable guardian as well as providing data that would equip organizations on how to become a less suitable target, are relevant to this subtheme. The premise of RAT is the existence of the three elements of a physical crime that should exist for a crime to take place. Essential concepts within the framework of RAT consist of the absence of a capable guardian, a motivated offender, and a suitable target (Kigerl, 2012). Effecting two of the three elements of the crime can provide an outcome that can be beneficial from a target position. Researchers have articulated that RAT is a theory that can be established to apply across multiple criminal activities (Leukfeldt & Yar, 2016). Providing security and awareness training can create a positive outcome in the creation of a more capable guardian as well as in regard to promoting attributes of a less suitable target for attackers. Traditionally, small businesses lack adequate resources and security and awareness training to effectively mitigate these threats (Ricci et al., 2019).

Training becomes an important security control to limit the motivated offender's path to access personally identifiable information. The virtual environment provides a link between time, space, the motivated offender, and the suitable target. Griffioen et al. (2021) proposed that the connection is made between the divide that consists of virtual cybercrime and physical crime, as this would also include the innovative internal applications that can be affected based on these factors leading to positive change that efficiently mitigates cybercrime. The capable guardian plays an important role in this intersection of time and space; as the guardian's capability is increased or decreased, the suitability of the target is increased or decreased, and it may affect the offender's motivations.

Subtheme: Vulnerabilities

One of the most difficult vulnerabilities to mitigate is human fallibility in the aspect of security. Social engineering is leveraged to bypass some of the most sophisticated technical controls that exist. Training, and a consistent awareness of attacker motivations that utilize different social engineering scenarios to enter a network by seeming to be a legitimate communication, is one that takes constant attention to adequately prevent compromise via this external threat. Sharing of information across organizations would provide threat intelligence to inform small businesses of the type of threat and how best to mitigate such a threat. When the topic of social engineering arose, six out of the nine participants regarded the topic as being one of the most frequent and serious threats that exist within the organization, as users are seen as some of the most vulnerable within an organization. Vulnerabilities are being discovered frequently within organizations. P1 stated that:

> For example, there is a new UPC vulnerability. Nobody would ever think that the UPC can be a mechanism used to infiltrate a network, as a lot of people employ UPCs, right? All these laptops and these devices internally connect to a power source that allows them to stay active when you know their actual electricity is down within their environment, and we just discovered the vulnerability.

P5 discussed the importance of monitoring downloads as it is a huge task to keep track of what is being downloaded and whether any malicious code exists within the downloaded applications. P5 also noted that it was confirmed by the cyber defense team that several of the downloaded applications did indeed contain malicious code. P6 also discussed that they have now found vulnerabilities within the patching system that is used to shore up vulnerable systems. P7 indicated that hackers are now leveraging the framework to locate attack vectors. P8 asserted that many developers are rushing applications to market, and security is not a priority in its production as the input fields of these applications are of major concern. P9 discussed that a big challenge is the remediation process, as there are many resources and workload owners, that it becomes a challenge to cover every aspect of security as there are new vulnerabilities at every turn. It is important to review the security assessments from deferent lenses to identify the gaps. P9 further explained that you could implement security controls, but nothing can really prevent a user from clicking on a malicious link.

The NIST documentation analyzed supported this theme regarding vulnerabilities that were deemed to be largely caused by human fallibility translated into how social engineering plays a significant role in the vulnerability of systems to obtain confidential information. The participants expounded on their opinions regarding this theme as their approach corroborated information gleaned from NIST 800 series documentation. NIST Framework 800-30, 800-39, 800-82, 800-161, as well as the NIST Management Framework that provides details regarding training, best practices, as well as a risk management framework to establish and sustain a secure cyber environment. When assessing the literature, social engineering techniques can be leveraged even though you have the most sophisticated controls to mitigate every level of external threat. Fellnhofer (2018) asserted that the most significant threats are executed in phishing attempts and other deceptive, socially engineered measures that prey on human propensities. Jensen et al. (2017) also pointed out that phishing is a social engineering attack that utilizes deception to gain access to sensitive information to benefit the deceptive party and is exceedingly difficult to identify. The unsuspecting user remains one of the weakest links in the cybersecurity network, as posited by Budzak (2016). Due to the rigorous attempts of utilizing social engineering to hack the user, its ease in execution, and the methods that are leveraged to entice the user to click on a compromised link, a rigorous training schedule should be implemented to keep the possibility of phishing attempts in a clear perspective. The correction of unwanted behavior is achieved through a rigorous system of testing that alerts an organization when an employee clicks on an email from a suspected external threat and has utilized social engineering techniques to enter the network (Prajogo et al., 2018). The training is often costly and not recognized as a practical and tangible return on investment for small businesses creating another expenditure that must be closely monitored and analyzed. Applying layers of security in the mitigation of social engineering techniques is warranted to improve small business cybersecurity defenses (He & Zhang, 2019).

From this perspective, the concepts of RAT, Cohen and Felson posit states that a change in any two of the three aspects of the crime regarding time and space is enough to create conditions for a less suitable target. Effecting two of the three elements of the crime can provide an outcome that can be beneficial from a target position. Researchers have articulated that RAT is a theory that can be established to apply across multiple criminal activities (Leukfeldt & Yar, 2016). Cohen and Felson’s (1979) RAT is leveraged in this study to explore issues that provide the impetus for cybercrime activities referencing an offender, a suitable target, and the absence of a control or mitigation technique. When reviewing the research, the researcher’s goal was to provide data that would measure the effectiveness of a more capable guardian while reducing the suitability of the targets to prevent, intervene, and respond to incidents (Choi et al., 2018). When adding in levels of security such as SATE, this could prove to provide another layer of security and awareness that would aid in the effectiveness of a more capable guardian leading to creating conditions of a less suitable target. However, these concepts do not provide solid evidence for the effectiveness of mitigating offender motivations. According to Kulig et al. (2019), the original concept of RAT did not provide an adequate definition of the attributes of a motivated offender, as Cohen and

Felson conceded this limitation and indicated future research was needed to understand offenders' motivation for the crime. Understanding offender motivations is a key element in understanding which organizations are more often targeted and requires further research to gain an adequate understanding of the phenomena.

Subtheme: Threat Motivation Deterrence as a Practice

In following the realm of the data derived from threat motivations and how an organization prepares for its deterrence, there is no set of rules or protocols amongst these organizations that are followed that seek to deter the motivated offenders' target aspirations. Also, there is no list of identifiable attributes of a motivated offender that can be utilized as a baseline in effecting offender motivations, Kulig et al. (2019) posited that the original concept of RAT did not provide an adequate definition of the attributes of a motivated offender. Therefore, to steer offender motivations into an agreeable result for the benefit of the target, those attributes are key in providing understanding going forward. Six of the nine participants mentioned some form of cybersecurity that they felt was key in deterring the threat motivations of attackers. P3 stated that "I would say following an industry standard was key in this effort." P4 discussed that security and awareness training, a great perimeter defense, as well as a good internal defense consisting of robust security controls that obfuscates organizational email addresses, were useful as sort of a threat motivation deterrence. P5 articulated that some of the name brands of the security devices would be a form of threat deterrence as attackers would see this as an organization that is serious about their level of security. P6 noted to provide a level of threat deterrence from an external source, "It's very hard to say…but a robust detection control infrastructure, as well as segmentation, are good principles to implement." P6 further articulated that prevention, testing employees, as well as having qualified cybersecurity analysts in adequate roles would do well in providing a threat deterrence that may steer organizations toward another target. P7 posited utilizing IP probing that can be leveraged to identify IPs which would lead to backlisting as well as referencing the MITRE attack framework as a threat deterrent. P8 proffered that any option that deals with varying layers of security increases the efficacy of their cybersecurity. Policies that consisted of 15-character passwords versus 8, a web application firewall (WAF), as well as network segmentation, as discussed by P6. In this theme, as the research has shown, there are no set of rules or standards to follow regarding threat motivation deterrence regarding motivated offenders as many varying controls were discussed by participants as defense in depth appears the consensus on this topic as more research is needed for better critical analysis of the phenomena.

The NIST documentation analyzed does not support this theme as an aspect of this study explores various strategies in relation to the conceptual framework that would provide new and innovative ways to enact a solution to aide in curtailing the motivations of the attacker, which is not a highly regarded phenomena for application nor study. This theme shifts the focus to the motivations of the attackers rather than a robust defense and training strategy as outlined in the NIST 800 series documentation. The participants expounded on their opinions regarding their approach to this theme, providing very little technology, policies, or procedures that provide any controls to mitigate the motivations of an attacker. This is in alignment with the findings within the literature where very little research is found as a course of action to be applied as a mitigation technique or control in regards to curtailing the threat motivations of an attacker.

When reviewing the literature, Kulig et al. (2019) articulated that the original concept of RAT did not provide an adequate definition of the attributes of a motivated offender, as Cohen and Felson conceded this limitation and indicated future research was needed to understand offenders' motivation for the crime as very little researched has been attributed to this phenomenon. To adequately provide an informed analysis of this theme, it would be deemed prudent to rely on data regarding the visibility of cyber victimization and the effect of the conditions on the motivated offender, and how to create an atmosphere to curb that motivation (Choi et al., 2016). When applying theories associated with RAT, there are spatial elements to a physical crime event and correlating conditions that must exist for the crime to be executed, as posited by Cohen and Felson (1979), consisting of a motivated offender, suitable target, and lack of a capable guardian. With the data provided, a good first step to understanding offender motivations and how best to curb those motivations, the suitability of the target, and how to propose actions to create a less suitable target may prove to be in the implementation of adding a layered prevention strategy whether those actions pertain to the environmental, spatial, or absence of any of the three required elements for a crime to be committed (Choi et al., 2018).

A key element of RAT, regarding this study, was to understand how to positively affect the aspects of the framework in ways that lead to the target becoming less suitable for an attack. Regarding this theme, how do cybersecurity analysts deter the motivations of an offender from an external threat perspective? One of the understood factors of criminology is the theory that crime will consist of three factors: motivation, opportunity, and the lack of a capable guardian (Cohen and Felson, 1979). These factors can apply in an individual incident as well as established trends. Derived originally to explain physical crimes, it is equally applicable across cyberspace (Grabosky, 2001). The motivated offender class is measured by the zeal they are willing to offend despite the negative consequences, often weighing a cost versus the reward factor. There is very little research that is definitive on how to best curtail those motivations of the offender. The motivations can be as simple as gaining a profit or a matter that may involve an instance where the convergence of time, space, and opportunity was suitable for committing the crime (Kulig et al., 2019). There are several mitigating factors as the motivated offender chooses a target. These factors consist of ease of access to the target, the ability to carry out the crime without being detected, the portability of the target, and the ease with which it can alleviate any evidence of the attack (Elmaghraby & Losavio, 2014). Going forward, these concepts require more research and examination as to how to best affect those attributes in a way that is beneficial in curbing the motivation of the offenders and creating conditions that make a target less suitable for an attack.

Theme 4: Assessing Threat Security Posture

A clear understanding is needed that identifies the status of an organization's enterprise networks, systems, and information based on an identified framework as well as their ability to adequately defend the organization's enterprise networks and react to situational changes. In the absence of a clear understanding of the security posture of an organization, cybersecurity analysts do not have adequate vulnerability data to defend their organizations against threats as well as against the increased risk of those threats materializing. For a small business to meet compliance, cybersecurity analysts must relay concerns and cybersecurity needs while remaining consistent in utilizing systems that ensure its infrastructure's confidentiality, integrity, and availability (Kakucha & Buya, 2018). This theme consists of three subthemes: lack of resources, training, and financial constraints (see Table 5).

Table 5

Subthemes for Assessing Threat Security Posture

	Interviews		Documents	
Subtheme	Count	References	Count	References
Lack of resources	4	23	2	7
Training	4	7	2	7
Financial constraints	5	23	4	7

Subtheme: Lack of Resources

Another important aspect of a small business cybersecurity strategy that affects the way cybersecurity analysts protect their organizations that arose from the study references a lack of resources. This subtheme is in alignment with the subtheme's financial constraints. The lack of resources of any organization is inextricably tied to the budget allotted for the quality of talent that can be recruited to help protect their assets form external cybersecurity threats. This aspect can play a role in the level of protection and how capable the organization is of defending itself from various external threats. P2, P3, P5, and P6 articulated that manpower was the greatest need when it comes to adequately protecting an organization form external cybersecurity threats. P1 described the lack of human resources in this way: “It is simply just the sheer amount of data that you have to kind of sift through to identify anomalies to identify threats and the like.” P1 further articulated that “it requires a lot of human resources … human eyes to go through the data effectively and efficiently within an acceptable timeframe, and therein lies the lack.” P3 stressed that staffing now is difficult just because of the way the world is right now. There are many openings, and everyone is looking for the best jobs, further creating a gap in hiring as the most experienced cybersecurity analysts are in high demand. P5 discussed that, in accordance with the lack of resources, there are a lot of processes that were not built to handle the volume of threats. There was also a lack of personnel who could adequately configure the tools to have adequate threat protection across the organization’s landscape. P5 also articulated that the organization lacked several key components of threat protection, referencing a lack of a DLP solution as well as a depleted GRC (Governance Risk and Compliance) team leading to cybersecurity analysts being overworked. P6 echoed the concerns of P2, P3, and P5, stating that experienced personnel was one of the greatest lacks of resources that they were experiencing. P5 also articulated that experienced personnel has the ability not only to protect against more complex threats but also have the knowledge to create contingency planning as well as utilize soft skills to foster relationships with partners, consultants, and supply chains.

This theme regarding a lack of resources is not alignment with any defense-in-depth strategy found in NIST documentation. The number of resources is inextricably tied to budgetary concerns and is different from organization to organization, as corroborated by participants in this study. The NIST documentation provides more of a focus on security best practices rather than budget allocation.

As the literature states, researchers have discovered a lack of resources in the small business cybersecurity domain (Almeida et al., 2018). As relayed in this study, one of the greatest concerns centers around the lack of personnel to adequately protect their organizations from external threats. Due to their small sizes, limited funds, and finite perceptions, small businesses often have access to a smaller pool of personnel and IT resources than their larger corporate counterparts creating a soft target perception amongst hackers, as reported by the NIST (2019a). The effect of lacking properly managed resources for a cybersecurity strategy can directly affect the business's finances, reputation, and objectives (Cunningham & Head, 2019). A key strategy in addressing the resources gap is to leverage the expertise of experienced cybersecurity analysts, which can help to quell some of the shortcomings of the small business by managing growth, technology, and innovation while understanding the escalating risks, implementing state-of-the-art security technologies, and assessing the threat landscape (Martin et al., 2017).

When leveraging RAT, this study explores the issues that provide the impetus for cybercrime activities referencing a motivated offender, a suitable target, and the absence of a control or mitigation technique (capable guardian) Cohen and Felson (1979). The absence of a capable guardian directly relates to the lack of available resources established in this study, more succinctly, being that of a lack of experienced personnel to adequately protect and defend an organization form external cybersecurity threats. The lack of cybersecurity resources is also apparent, as well as the lack of trained cybersecurity analysts that understand how to provide a coordinated incident response effort and a plan of action that has been tested on a scheduled basis for readiness to effectively mitigate cyber threats (Osborn & Simpson, 2017). There is a limit to the amount of data an organization can sift through to adequately identify the threats from the alerts. Automation is paramount in the prevention of external cybersecurity threats and provides a new pathway for the next evolution in the prevention of external cybersecurity threats hinged on AI (Lino et al., 2019). Leveraging technologies that can be automated while providing adequate training for these technologies allows cybersecurity analysts to focus more on the real threats capitalizing on machine learning to process larger amounts of data in a shorter time period. This process could prove to be very useful within a small business threat detection strategy allowing resources to be better allocated where needed.

Subtheme: Training

Training is a key aspect of any small business cybersecurity strategy. Training is the cornerstone of any cybersecurity program as it allows cybersecurity analysts to gain the knowledge to execute technical and nontechnical processes properly. For the organization to adequately leverage and manage all aspects of people processes and technology, frequent training should be a part of every cybersecurity strategy. Training must be leveraged to adequately identify and prevent threats from compromising an organization. This study emphasizes training regarding security and awareness, as social engineering was regarded as the most prevalent threat established by the participants in this study. When questioned about the most effective ways to prevent cybersecurity attacks, four of the nine participants specifically articulated that training was paramount in this initiative. P4 indicated that:

> We can get the bodies in, but if they are inexperienced or are not used to working with technology and there is a ramp-up period…we will experience a lot of inefficiencies. Once they become adept and gain the experience, they can put a better methodology in place to run their tools.

Cybersecurity analysts gained experience as a common practice by adhering to continuing education and applied on the job training keeping them up to date regarding the latest threats and prevention techniques. P6 further articulated that to protect your systems from external cybersecurity threats, you must train your staff. One of the most efficient ways to protect against cyberattacks and also all types of data breaches is to train employees on cyberattack prevention and to keep them informed on current cyberattacks, including security and awareness training. P8 articulated that the plan is to leverage the training to stay one step ahead of the hackers. P9 stated that "To ensure users are well-trained, security and awareness training is something you must have in place."

Three of the remaining participants discussed the issue of a lack of adequate training within their organizations. P1 noted that they very seldom seek new training in the face of new threats. P5 articulated that a lot of the processes were inadequate and not setup to handle the volume of threats. P9 discussed that the level of knowledge regarding basic security is rather shallow for new graduates. They possess the knowledge to develop a system but lack the skills to develop it securely. The knowledge of networking and TCP/IP is basic at best.

NIST documents from participant interviews corroborate their approach to this theme as specific security and awareness best practices are outlined in several NIST 800 series documentation. The documents address integral aspects of a security and awareness program as well as the importance for organizations to train and equip end-users with the requisite knowledge and awareness to be able to combat, mitigate, as well as recognize security threats. NIST Framework 800-30, 800-39, 800-82, 800-161, as well as the NIST Management Framework, provides details regarding training, best practices, as well as a risk management framework to establish and sustain a secure cyber environment.

When reviewing the literature, small businesses lack adequate resources to provide robust security controls and comprehensive cybersecurity training programs (Ricci et al., 2019). Small businesses must find new and innovative ways to adequately train their employees, as this aspect of cybersecurity is literally a cost center that must be funded. Systems that consist of endpoint protection, threat detection, threat prevention, incident response, and training required for effective, efficient mitigation and eradication of threats are expensive and play a significant role in how small businesses approach cybersecurity hygiene (Raghavan et al., 2017). The most prevalent threat identified as social engineering in the form of phishing attempts in this study requires specialized training. The SATE program provides data on each user that can be modified to fit each user's behavioral pattern. Over time, the program allows the user to effectively identify threats from external sources, thereby decreasing human risk to the organization (Jackson, 2018). The SATE training is not foolproof and requires constant monitoring and testing to achieve the goal of alerting users to what nefarious email campaigns may enter their inbox, setting the stage to identify the threat and report it.

The specific concept of training is not addressed in the framework of RAT; however, the rigorous training aspect of cybersecurity can lead to positively affecting the crime triangle by creating a more capable guardian leading to a less suitable target that, in theory, leads to dampening the motivations of the offender and would likely cause the offender to choose a less suitable target to attack due to resource and time constraints. This new infrastructure undoubtedly will require smaller businesses to make critical decisions on training for technical and security and awareness-based programs within their organizations (Humaidi & Balakrishnan, 2018). The more cybersecurity analysts are engaged and provided with training to be successful may result in more significant dividends on the backend resulting in innovation and better protection of data as trained cybersecurity analysts will better understand the infrastructure, its threats, and how to apply effective strategies based on the current environment (Yoo et al., 2018). Wolverton and Stevens (2019) acknowledged that some studies demonstrate that these are effective methods in mitigating susceptibility to phishing attacks; however, other studies have shown that one-quarter of the participants were just as susceptible to phishing attacks after receiving security and awareness training. In the future, more study is needed on how the motivations of offenders can be properly understood and leveraged to produce a desired outcome.

Subtheme: Financial Constraints

An organization has many different strategies that are based on its ability to provide the finances to accomplish them. The tone of this study, provided by the participants, references that the C suite of employees drives the finances and what percentage of the budget will be allocated for each aspect of security. Cybersecurity analysts must have a clear understanding of what the strategy is and what aspects of security require the lion’s share of the budget to adequately mitigate any gaps in the security posture. Constraints must be placed on people, processes, and technology to adequately disseminate the finances across the organization to prevent an excess of resources in areas that are not cost-effective. At some point, a risk analysis should be completed to get a comprehensive picture of the costs to protect each asset. P4, 6, 7, 8, and 9 discussed the financial constraints that are managed across each of their organizations. P4 articulated that when dealing with C-level executives, you will run into financial constraints, and cybersecurity analysts must sell them on how those constrains should be managed. We must identify the expenditures needed per asset. The biggest challenge is being able to communicate that information to the C suite and getting the funding needed to purchase the tools to properly implement the strategy. P6 stated, “In your organization, you must understand risks and not only cyber risks but other types of risks as you must have a comprehensive way of looking at risks within your organization.” P7 articulated that:

> I am not sure I can use the term constraint…its available financial resources based on the goals and objectives because each department may be allocated a certain

> amount of funding for their initiatives, and once the funding is exceeded, you can’t go any further. It is more or less a financial commitment that is available to that particular department. It’s a challenge because it depends on who the department head is or management … to know and identify those particular products, tools, or resources that are needed within that budget. It comes down to tools I can purchase and tools I can’t purchase, so it will always be an economical or financial decision. If I were able to purchase any tool and budget wasn’t a concern, we would still not be fully protected.

P8 discussed that typically with the C level, there could be challenges because they are more focused on the bottom-line and compliance issues and not necessarily real-world implications, as budget is one of the biggest issues when it comes to getting things mitigated. P9 also articulated that the level of protection needed to adequately protect an asset ultimately comes down to budget. P9 further articulated that a risk assessment is required to understand if the security controls that are being added are justifiable from a financial perspective, as in some instances, the control is more expensive than the asset itself. In this instance, it makes no sense to protect an asset of this kind, and we would just need to assume the risk. The challenge is understanding what needs protection and how much is needed to protect the asset, as well as the cost of the asset in the case an offender gets his hands on the asset. All nine participants indicated the importance of understanding the risks associated with each asset and a comprehensive understanding of the costs needed to adequately provide a control to mitigate that risk versus the asset value. These aspects of security are required to be understood by cybersecurity analysts as these principals are at the forefront of budget allocation and the molding of financial constraints.

This theme regarding financial constraints is not alignment with any defense-in-depth strategy found in NIST documentation. The number of resources, whether constrained or unlimited, is inextricably tied to C-level priorities and is different from organization to organization, as corroborated by participants in this study. The NIST documentation provides more of a focus on the security best practices rather than budgetary constraints and the leadership of the organization.

As the research has shown, when navigating a small business, there are several concerns when outlining a cybersecurity strategy and addressing policy initiatives. There are three main areas of concern when applying a finite set of resources: staffing, financial, and resource deficits (Selznick & LaMacchia, 2018). As derived from this study, financial constraints are of major concern when addressing budget allocation and where the dollars will be spent to comprehensively protect their organization. The Ponemon Institute (2019) reported that small businesses are at greater economic risk per employee than larger corporations of 500 or more as their losses were comparable in dollars lost per employee, thus creating a more significant financial impact due to their smaller size, a lesser amount of capital, and finite resources. Small businesses must make applicable data-driven decisions and create standards that provide a picture of what is needed to better prevent external cybersecurity threats when applying budgetary constraints (Kobe & Schwinn, 2018). Mistakes made within a small business are further magnified as they do not possess the financial capital of their larger counterparts and have to be more accurate in their risk analysis and asset identification.

When applying the concept of RAT, financial constraints affect two of the three main tenets of RAT. One of those concepts of RAT pertains to the effect that financial constraints have on the ability to increase or decrease the capabilities of the guardian. One of the key aspects of RAT is to increase the capabilities of the guardian to provide an improved outward-facing attribute of security while becoming a less suitable target (Hawley, 1944). The lesser the constraint, the better equipped the small business can be to provide a more capable guardian within their organization, such as better people, processes, and technologies. When reviewing the research, the goal of the researchers was to provide data that would measure the effectiveness of a more capable guardian while reducing the suitability of the targets to prevent, intervene, and respond to incidents (Choi et al., 2018). The capable guardian provides a constant presence consisting of individuals whose very presence deters criminality, provides an avenue for a speedy recovery, or sanctions against the offender that can be applied in cyberspace as posited by Hawdon et al. (2017). The other concept that can be directly affected by financial constraints is the ability to create conditions to make the target suitable by providing more resources to thwart the motivations of the attacker. In theory, providing more resources would build a more stringent security posture that creates conditions to lessen the suitability of the target. Manifesting conditions to achieve an even higher level of capability, lessen the suitability of the target, and how to propose actions to create a less suitable target may prove to add a layered prevention strategy whether those actions pertain to the environmental, spatial, or the addition or subtraction of any of the three required elements for a crime to be committed (Choi et al., 2018). The greater the ability of an organization to affect the concepts of RAT, the better chances of creating favorable conditions in the mitigation of cybersecurity threats.

Theme 5: Address Risk and Prevent Attacks Related to External Threats

Cybersecurity analysts cannot address risks properly without first understanding the value of their asset and the cost of the control to protect that asset. A misallocation of resources can leave some assets of very little value secure while the sensitive PII is left vulnerable to attack. This could also lead to reputational damage as the small business could be seen as irresponsible for not executing due diligence regarding the proper analysis that would have mitigated such an attack. This theme includes three common subthemes: asset monitoring and management, threat intelligence, and varying routine activities as a practice (see Table 6).

Table 6

Subthemes for Ability to Address Risk and Prevent Attacks Related to External Threats

	Interviews		Documents	
Subtheme	Count	References	Count	References
Asset monitoring & management	7	14	3	11
Threat intelligence	2	4	4	10
Varying routine activities as a practice	4	4	3	7

Subtheme: Asset Monitoring and Management

A clear view of the organization's structure, responsibilities, people, and assets is needed to quantify risks to protect the organization form external threats adequately.

Seven of the nine participants discussed the importance of asset management and monitoring regarding external threat prevention. P1 stated,

> We are big on utilizing a passive asset monitoring solution…Essentially, our role is to analyze an individual asset to identify its vulnerabilities based on industry data gathered regarding the asset. The data would consist of things such as the operating software, version, and model of the device, as well as system updates...We also analyze the environment that surrounds the asset to get a better understanding of how it would function to obtain a total understanding of what its behavior is predicated on.

P4 discussed that when establishing methods to protect an organization from external threats, whether large or small, it depends upon the assets you are trying to protect. The value attached to the assets you protect defines the controls that you implement. When assessing the external threat, it is prudent to try and discover ways they can enter your network via technology, people, or processes. This begins with understanding exactly what is lost and when to assess who or what is assigned that responsibility to act. P5 also articulated that "we have a specialized asset management IoT sector whereby we monitor client's environment to allow them to strategically place their assets into categories … to understand the vulnerabilities on the network form a layer two perspective." P6 noted that everyone must take part in protecting the organization. It is very important to monitor the level of preparedness and prevention within the organization. P9 articulated that an aggregation of different standards, most importantly continuous monitoring, no matter which standard you use, it is imperative to look at the assessments through different lenses to understand where the gaps are. Different workloads require varying levels of assessment and asset management.

Support for this theme is addressed in the NIST CSF, which provides organizations with a risk-based compilation of guidelines that can help to identify, implement, and improve security best practices. The NIST CSF does not introduce new standards or concepts; however, it applies and integrates practices that have been created by organizations such as NIST as well as ISO. The NIST CSF provides five core functions that are comprised of Identify, Protect, Detect, Respond, and Recover to aid in risk management. This theme would be categorized in the “Identify” function of the framework, which entails how to manage cybersecurity, risks to systems, assets, data, and capabilities. The framework recognizes that there is no one-size-fits-all approach to managing cybersecurity risks as organizations incur unique risks, varying threats, varying vulnerabilities, as well as varying risk tolerances; however, these are the strengths of the framework. The application of this voluntary framework provides guidance as to its efficacy, touting that it helps businesses of all sizes to better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The NIST CSF overall goal is to improve risked-based security (FTC, 2022).

When identifying key aspects of the literature, one of the most important duties of cybersecurity analysts is asset monitoring and management. If an organization doesn’t understand the scope of assets under its control, it cannot properly protect those systems or identify their importance. This theme is confirmed in the literature as several studies have touted that understanding asset management can provide invaluable information as to how to create strategies to properly protect your systems. NIST SP 800-61 Rev. 2 can be utilized to effectively provide an outline to identify its most valued assets and provide a strategy to protect its infrastructure (NIST 2018). In the grand scheme of asset management and monitoring, PII is the most important of all assets to an organization. Consumer PII is the most critical asset of each organization (Aishwarya et al., 2018). Bauer and Bernroider (2017) noted that senior-level executives play the most significant role in supporting the development and implementation of the cybersecurity program and its strategic purpose, which encapsulates policies and procedures created to protect organizational communications, assets, and systems from external as well as internal cybersecurity threats. When identifying one of the most prevalent cybersecurity threats, as outlined in this study regarding phishing, Korpela (2015) pointed out that the purpose of a security and awareness training initiative is to bring a security mindset to end-users alerting the culture to the dangers that plague information security assets while promoting the adoption of best practices which translate to another layer of protection for cybersecurity resources.

When applying the key concepts of RAT to asset monitoring and management regarding the ability to affect change in the capability of the guardian as well as decreasing the suitability of the target, essential concepts within the framework of RAT consist of the absence of a capable guardian, motivated offender, and a suitable target (Kigerl, 2012). Providing accurate risk assessments can aid in the process of creating a more capable guardian as this action identifies asset values and which resources are needed to adequately provide compensating control against the risk of creating a less suitable target (Sravanthi & Nisha, 2021). The goal of the researcher was to provide data that would measure the effectiveness of a more capable guardian while reducing the suitability of the targets to prevent external cybersecurity threats (Choi et al., 2018). In this instance, providing adequate risk assessments can add to decreasing the suitability of the target as the assets are adequately valued and the proper compensating controls are applied. Conditions regarding the suitability of the target will be in direct response to compensating controls implemented to enhance guardianship, presumably leading to increasing the capability of the defender (Choi et al., 2016). In the aspect of the motivated offender, there is not enough data regarding attributes that would assuredly affect the motivations of the attacker; however, the added levels of security may prove to be effective in steering an attacker to another target due to the innovations of cybersecurity analysts. Kulig et al. (2019) posited that the original concept of RAT did not provide an adequate definition of the attributes of a motivated offender to analyze any effects of deterred motivations. The concepts of RAT can be applied to better understand how a physical crime translates to a virtual crime simply by increasing and decreasing attributes regarding asset monitoring and management. Cybersecurity analysts should embrace the concepts that entail the suitability of the target and the increase or decrease in the capability of the guardian while focusing on asset monitoring and management to provide information for strategies going forward.

Subtheme: Threat Intelligence

Gaining an adequate perspective of the threats that could potentially attack small businesses is key in correctly identifying threats and providing a comprehensive and planned response. Threat intelligence is dependent upon the sharing of information across networks to provide a measured response that can be brought online quickly to thwart the next malicious threat and provide a feedback loop to better prepare and respond to the next threat. Initial attacks and prospective threats can be identified with a threat intelligence capability that provides detailed information that can be useful (Han et al., 2021). In the face of new and emerging threats, threat intelligence seeks to reduce the time between compromise and detection (Tounsi & Rais, 2018). When asked about the improvement of inefficiencies, a conversation regarding threat intelligence emerged. P1 stated, "We ingest a lot of cybersecurity feeds, threat analysis, and a lot of things of that nature for our security appliances as we just hired a threat intelligence researcher." P9 discussed that they indeed utilize a myriad of tools that leverage the latest technologies to better understand user behavior that entails patterns of access that are heavily driven by the application of machine learning. P2 explained that threat intelligence is centered around the prevention and identification of the source as well as focusing on the threats within the environment, which consists of parsing through a lot of data that may require added resources to parse efficiently.

This theme regarding threat intelligence is not directly in alignment with any defense-in-depth strategy found in NIST documentation; however, threat intelligence is a new and emerging aspect of the cybersecurity framework that will become increasingly important as new models for security are formulated. Intel, in accordance with NIST CSF, has implemented a Threat Intelligence category, modified tiers, as well as altered the Core to better match their business environment needs. After these modifications, Intel initiated a four-phase process for the utilization of the framework. After applying the framework, Intel touted that the framework could provide value to the largest of organizations and has the potential to transform cybersecurity on a global scale by accelerating cybersecurity best practices (NIST, 2021).

As validated by the literature, providing another level of security within an organization is very much an accepted practice by cybersecurity analysts. In the absence of informed threat intelligence and analysis from various sources for threat identification, a cybersecurity analyst cannot properly provide strategies to mitigate external threats based on the current threat landscape. The inability to provide an accurate landscape of threats that are pertaining to the organization can invariably lead to an inordinate number of unidentifiable attacks leading to a higher instance of data breaches (Gwebu et al., 2018). Threat intelligence platforms provide a source of data that can be leveraged to provide insight into the next generations of threats (Gong & Lee, 2021). Threat intelligence can be constructed to fit each organization and provides a level of operational efficiency and acceptable response times that depends on automated and real-time data (Rowley, 2019). Organizations provided information that in the age of new and emerging threats, APTs utilize certain tools, tactics, and procedures (TTPs) that could then be identified via threat intelligence (Bromiley, 2019).

In contrasting the concepts of RAT, Cohen and Felson (1979) articulated that RAT directly applies to concepts where the motivated offender, lack of a capable guardian, and a suitable target all converge as they must be present before a physical crime can take place. In a virtual environment, these factors are linked by time and space.

However, Reyns et al. (2011) noted that the application of the network-based crime triangle displays how RAT can be expanded to include crimes that take place with distance as a factor in which motivated offenders and suitable targets do not intersect at a physical location. In this instance, the ability to provide threat intelligence plays a role in the guardian increasing their capability, therefore, decreasing the suitability of the target. The need to supply a capable guardian with tools to effectively execute their primary function in the crime triangle, as well as how to manifest conditions to achieve an even higher level of capability, the suitability of the target is decreased (Choi et al., 2018). Leveraging cyber threat intelligence (CTI), in conjunction with defense in-depth strategies, decreases the likelihood that an external threat can achieve a successful attack. Decreasing the attack footprint, as well as lowering attacker opportunities, reduces the likelihood of victimization (Pratt & Turanovic, 2016). Implementing a layered defense with technologies such as threat hunters with next-level capabilities reduces the likelihood of an attack (Hawdon et al., 2020).

Subtheme: Varying Routine Activities as a Practice

Small businesses require innovative strategies to provide a high level of security that would aid in the protection of their assets. Keeping the costs of protecting these assets manageable is key to the viability of the organization. The understanding of the importance of varying the routine activities of personnel was accepted by all participants; however, not all provided a procedure or protocol that would ensure that these strategies were being implemented and practiced as a "defense-in-depth" strategy within their organizations. Participants 1, 2, 3, 6, 7, and 8 discussed that varying the routine activities of personnel was not practiced at their organization. P1 stated, “We have not implemented any strategy of the sort based on the nature of the company. We are not all stationary, and many of us work remotely, as I don’t see this being utilized within our organization.” P2 and P3 agreed that they saw no official implementation of a procedure that would vary the routine activities of their personnel. P6 opined that in most cases, it would not be a good idea to vary the routine activities of people, as for some organizations that are plagued with a high turnover rate, this could prove to be dangerous as you are staggering personnel that is highly skilled with employees that are less skilled. You may have highly trained personnel who are familiar with the system, infrastructure, as well as the organization, as this would leave a gap in coverage. You also may have individuals who have seen those types of threats before within the organization that would be key in mitigating a threat that has now been routinely routed to another area where the protection is not as warranted. Creating a lot of variations in roles, people, and responsibilities may be a dangerous endeavor. P7 noted that we do not vary the routine activities of personnel; however, we do provide scannable badges that restrict the routine activities of those who are not authorized to access sensitive areas. P8 explained that they focus on the routine habits of the attackers and utilize strategies that can identify those salient points within a network, as no real discussion that covers the routine activities of personnel has taken place. Participants 2, 4, 5, and 7 utilize some form of a procedure where they vary the routine activities of their personnel to provide full coverage of their networks to have “eyes on glass” at all times.

This theme regarding varying the routine activities as a practice is not alignment with any defense-in-depth strategy found in NIST documentation; however, varying the routine activities of people, processes, and technologies is being explored in this study. This study may provide greater insight into how the aspects regarding the conceptual framework of RAT, in comparison to virtual crimes, can be leveraged in order to create viable cybersecurity standards to aid in cybersecurity mitigation and prevention. These aspects are novel, and their continued analysis, as applied to virtual crimes, may foster innovative ways to approach cybersecurity controls and techniques to secure systems form external cybersecurity threats.

When comparing the literature regarding this theme and reviewing the interviews, cybersecurity analysts have not provided much data that led to the implementation of varying the routine activities of personnel. In some instances, applying data from other subsets may prove beneficial in the areas that have not provided significant data to analyze. It should also be noted that generations of victimologists have integrated lifestyle exposure theory and RAT into what they now call LRAT of criminal victimization, highlighting the importance of an individual’s lifestyle and routine activities in generating opportunities for victimization (Messner et al., 2007). A discussion that surfaced regarding the lack of experience of some personnel could prove detrimental when varying the routines of people and processes. The lack of acquiring highly trained cybersecurity analysts is inextricably tied to costs. In agreement with Selznick and LaMacchia (2018), Watad et al. (2018) articulated small businesses must understand that cybersecurity is regarded as a cost of participating in commerce and a requirement that deserves time and effort managing. Mithas et al. (2018) articulated a global shortfall of about seven million qualified cybersecurity professionals, which provides the impetus for small and medium-sized businesses to incur a lack of human capital to thoroughly research the broader issues that plague cybersecurity to increase security while lowering costs.

The concepts of RAT identify that varying the routine activities of the spatial elements of a crime, with the focus on the target institution, assumes that an offender with the means, motive, and opportunity can successfully commit a crime when the conditions are favorable, as posited by Cohen and Felson (1979). The theory also assumes that the victim plays an intricate role in choosing to be victims by not placing themselves in a position where crime can be committed against them. This theory provides an interesting perspective on the varying factors of victimization and prevention strategies that may well translate to cybercrime. When applied in this context, varying the routine activities of the elements of the crime could prove beneficial when choosing strategies to mitigate the threat. By applying RAT principles, IT cybersecurity analysts may have adequate leverage in contributing to reducing the risks associated with victimization-related events (Choi et al., 2016). When providing strategies that vary, the routine activities of personnel can provide strategies that increase the capability of the guardian and create more obscurity within a system, hindering the external attacker's ability to gain knowledge within a network. After highly publicized data breaches experienced by major corporations where millions of dollars in revenue and regulatory fines in the billions were lost, cybersecurity analysts adopted new strategies to counter cyberattacks known as “moving target defense” (Ghourab et al., 2019). These new and innovative approaches to cybersecurity can offer small businesses the leverage needed to find affordable strategies to increase their overall security posture. More innovative strategies which allow cybersecurity analysts to think outside of the box are introduced in the form of cybersecurity analysts adopting “goal protection” that, in essence, purposefully reconfigures the IT landscape to protect against identified attacks (Park et al., 2018). In this realm, reviewing cybercrimes through the lens of RAT offers a unique perspective on mitigating cybercrimes in small business organizations. When reviewing the research, the researcher’s goal was to provide data that would measure the effectiveness of a more capable guardian while reducing the suitability of the targets to prevent, intervene, and respond to incidents (Choi et al., 2018).

When small business cybersecurity analysts become more engaged and are provided with adequate training, this may result in more significant dividends on the backend, fostering innovation and better protection of data as trained cybersecurity analysts gain a better understanding of the infrastructure, its threats, and how to apply effective strategies based on the current environment (Yoo et al., 2018).

Theme 6: Centralizing Communication to Provide Perspective on Threats

Communication within an organization across departments must follow a specific chain of command to be effective and allow for the proper dissemination of information that may be pertinent to an entity within the organization. A disruption in this flow of information causes concerns that can leave a small business ill-prepared to carry out its business goals and directives. Cybersecurity analysts deal with the dissemination of information daily, and if that function is disrupted, they cannot effectively carry out the mission of protecting the most critical assets within the organization. Cybersecurity analysts are tasked with the responsibility of the transmission of critical information to the correct individuals regarding specific cybersecurity incidents in a timely manner. This theme consists of three subthemes: C-level buy-in, lack of communication, and analysts' views of cybersecurity strategy (see Table 7).

Table 7

Subthemes for Communication Across Departments to Provide Perspective on Threats

	Interviews		Documents	
Subtheme	Count	References	Count	References
C-Level buy-in	9	29	3	11
Lack of communication	1	1	4	7
Analyst's views of cybersecurity strategy	7	15	3	6

Subtheme: C-Level Buy-In

When providing strategies to protect a small business properly and effectively, C-level buy-in is of the utmost importance. Budget is one of the most significant challenges to a small business cybersecurity strategy. Radziwill and Benton (2017) asserted that budget was a perpetual concern amongst small businesses that seek to implement efficient cybersecurity methods and protocols. All nine participants provided input on how C-level buy-in plays a significant role in the direction of their cybersecurity strategy and, ultimately, their cybersecurity posture. Cybersecurity analysts are tasked with the duty of providing a clear understanding of the threats their origination faces and whether that threat is worthy of receiving the needed resources to adequately protect the asset above other pressing concerns. Participants 1, 2, 4, 5, 6, and 7 discussed that the C-level buy-in was key in the implementation of cybersecurity initiatives and often was an arduous task to gain buy-in for the projects they deemed necessary to provide comprehensive cybersecurity. P1 explained when it comes to gaining C-level buy-in quickly, it was more obtainable from a small business perspective versus their larger counterparts. He outlined a process that, upon his hire, he was highly scrutinized to be sure he was a proper fit for the organization, which leads him to believe that C-level trusts their analysts a bit more due to the vetting he received. P2 stated,

> The biggest concern of the organization will always pertain to the budget. Another concern of the organization was who was going to be responsible for the new technology once purchased. … Who would have the technical capabilities to adequately operate and support the resources? Should we purchase an open-source product or a vendor-related product that offers support? We do these things to show the C-level where the value is in the product.

P4 explained that you typically run into the issue regarding financial constraints when seeking C-level buy-in. He further elaborated that they must provide information that shows visibility into the cost per asset that they are trying to protect, as the greatest challenge is being able to convey this information to garner the funding needed to purchase the tools, implement a methodology, or obtain the appropriate headcount needed to protect the asset. P5 explained that C-level was not very skilled or effective at communicating the aspect of risks to the organization as some of their backgrounds did not provide the proper understanding of how to communicate or understand those concerns in the form of risks to the organization. He further explained that a lot of the communication was provided to C-level in the form of a dashboard. P5 also stated,

> It was really hard to get any feedback as we got as far as the information being communicated through the dashboard. We were not sure if this was enough or if it was telling the story you kind of want to tell, especially to C-level. … There was more of a let's try to make C-level happy rather than to educate them on the … you know this type of security that we should try.

P6 explained that one of the most important things is to connect the dots between business strategy and the security program, as these two departments seem to speak different languages, as the results for the technology security team are quite different from the project and business goals. He further explained that it is important to provide C-level with real-life examples as some are not acquainted with the technical aspects of the information. All nine participants discussed the importance of achieving C-level buy, and one of the most effective ways to relay this is by providing a method that outlines the cost of the asset being protected and the cost of the control to mitigate its vulnerability if exploited.

NIST documentation does not exclusively outline C-level-buy-in as a defense-in-depth strategy in support of this theme; however, C-level-buy-in is an integral part of providing a comprehensive and strategic model for the implementation of cybersecurity for small businesses, as well as providing careful and thoughtful decisions as to the direction of the organization's security program which allows small business to compete with their larger counterparts in protecting their organizations.

As validated by the literature, cybersecurity resource allocation in small businesses is a delicate balance between the C-level executives, which their buy-in is a significant factor in approving cybersecurity initiatives, and its perception as some view its function as a cost rather than a needed investment that protects their organization from company ending data breaches and liabilities (Raghavan et al., 2017). The role of cybersecurity, C-level buy-in, management, and its implementation within a small business must be shared by all, from the unheralded cybersecurity analyst to the Chief Information Security Officer of the organization (Rothrock et al., 2018). In a small business, the expanding landscape of vulnerabilities when obtaining new and improved technologies to maintain business relevancy and sustain growth is no different than in larger corporations; however, smaller firms must find innovative ways to maximize the buying power of every dollar through common sense cybersecurity strategies (Markey, 2018). Small businesses must be united in protecting their organization from varying levels of threats, especially techniques that require the entire organization to play a role in the reporting and mitigation of threats. Understanding the threat of social engineering techniques requires an organization to present a united front amongst C-level executives to induce buy-in and promote security and awareness (Bada & Nurse, 2019; Hwang et al., 2017).

The concepts of RAT do not directly relate to C-level communication and buy-in; however, obtaining C-level buy-in can result in creating a more capable guardian in the form of improved security controls as well as improving the security posture of an organization which leads to a less suitable target. Achieving C- level buy-in affects two of the three main elements of RAT. Effecting two of the three elements of the crime can provide an outcome that can be beneficial from a target position. Researchers have articulated that RAT is a theory that can be established to apply across multiple criminal activities (Leukfeldt & Yar, 2016). One of the key aspects of RAT is to increase the capabilities of the guardian to provide an improved outward-facing attribute of security while becoming a less suitable target (Choi et al., 2018). Cybersecurity analysts provide an important role in C-level buy-in as they must effectively communicate complex issues that directly affect the cybersecurity posture of their organization, indirectly affecting the data needed to apply the concepts of RAT. Hawley (1944) touted that increasing the capability of the guardian while making the target less suitable contributes to the frequency of crime rates allowing cybersecurity analysts to provide strategies that would positively affect data breach rates in theory. C-level buy-in is a very critical step in garnering the security resources needed to adequately protect small businesses as well as improve communication across departments.

Subtheme: Lack of Communication

Understanding how to relay information to the varying departments within an organization is key to the overall success of the small business. Different departments require varying ways of communicating. Many departments require communication to be formulated around the cost related to the small business, while others require technical jargon for that department to fulfill its business-related goals and strategies.

Cybersecurity is no different. Communication that has been formulated to inform the cybersecurity department requires a language of its own. In some cases, it can be highly technical, and not every department will understand the message being relayed nor be equipped to gather the information needed as to what their role is to ensure the protection of the organization. It is important for the cybersecurity analyst to bridge this gap and take complex ideas and outcomes of a technical nature and distill them so that they can be consumed by each department. All nine participants discussed that a lack of proper communication across departments and organizations impedes the progress of any small business, its goals, and its cybersecurity strategy. P5 explained that there are many gaps between personnel ranging from the CISO to the legal officer, including the rest of the board. P5 further elaborated that their new CISO was just not an effective communicator. The background the CISO possessed was centered around vulnerability management and was not very conducive to a conversation that centered around risks. The ability to effectively communicate the issues within the organization regarding cybersecurity risks to C-level personnel was a challenge. P6 explained that one of the most important things was to connect the dots between departments as often departments speak two totally different languages. P6 also stated that information was relayed in the form of a cybersecurity presentation to the board that contained data from the technology security team that was altogether different than data regarding projects and business goals. P6 found the utilization of heat maps and colored graphs highly effective in relaying messages to the C-level personnel. P7 explained that when garnering C-level support, there are varying viewpoints and recommendations being considered that are often not compatible with the direction of the organization. P7 further opined that it is important that management allows varying elements, movements, decisions, and directions from varying teams, as this can lead to changing the overall direction based on recommendations. P8 explained the communication gap as a matter of different viewpoints as the C-level remains focused on the narrative of expenditures and compliance due to the auditors and not necessarily the real-world implications of those decisions that guide the security posture of the organization. P1 was a bit of an anomaly as the participant regarded upper management and their ability to communicate very highly. P1 stated, “If there were good ideas that would benefit the organization, upper management would run with it.”

NIST documentation does not outline the lack of communication as a defense-in-depth strategy in support of this theme; however, communication is an important part of providing cybersecurity for a small business as well as educating all stakeholders on the importance of providing clear and concise communication in protecting their organizations. An important aspect of communication, not necessarily in regards to C-level executives’ direction for the organization, but on an incident response level, can be leveraged to provide a model for comprehensive communication within an organization as well as to external parties. NIST Frameworks 800-53, as well as 800-171, covers aspects of incident response as all participants provided an approach regarding this aspect of security and considered it key in protecting their organizations.

When perusing the literature, communication is key when relaying information that must be consumed quickly and disseminated to every department. The organization must be on the same page to adequately provide the protection needed to mitigate threats. NIST (2018) best practices dictated that organizations require a predefined plan of action to handle incidents in an incident response plan. A well-developed incident response plan prepares the organization to pursue efficient response times, provides a call tree for seamless communication with backup employee roles, and adequate procedures while carrying out attack scenarios and training drills, as purported by Greene et al. (2017). Wertheim (2019) articulated that incident response is often viewed as a cost center instead of a benefit to the organization that protects the bottom line. C-level executives share this culture and believe that incident response costs are better served by allocating funds to invest in time, money, and people who drive economic growth rather than optional response efforts. An excellent tool for relaying information to each department is industry standard tabletop exercises that allow small business owners to identify vulnerabilities in the communication process and identify gaps in preparedness while strengthening the response teams' ability to carry out their duties under stressful circumstances. Tabletops can involve anyone in the organization to participate in a real-world mock attack bridging the communication gap across the organizations. Tabletops can also include other organizations, such as legal services, third-party vendors, and other small businesses. Small business cybersecurity leaders should construct effective communication channels that alert the small business leaders of their threats in the future (James, 2018). Cybersecurity analysts cannot bridge the communication gap without having a clear understanding of each department's business goals and how they defend those goals from a threat and risk perspective.

The communication gap that exists within an organization is not directly tied to the concepts of RAT. However, creating better communication channels internally as well as externally affects all three aspects of RAT indirectly, thereby leading to a more capable guardian, a less suitable target, as well as curbing the motivations of the offender. Essential concepts within the framework of RAT consist of the absence of a capable guardian, a motivated offender, and a suitable target (Kigerl, 2012). When creating external sources of improved communications provides small businesses with information that will have been disseminated across organizations containing pertinent data describing the current tips, tactics, procedures, and tools utilized to attempt to penetrate small businesses' networks. Young and Yung (2017) described a lack of innovative strategies to maintain adequate protection against threats that embolden hackers to exploit systems. The communications can then aid small businesses in quickly identifying threats and provide adequate mitigation controls that can be shared across small businesses. As a result, this would make the target less suitable for the motivated offender and possibly lead to curbing the motivations of the attacker. When applying the theoretical framework of RAT while referencing the data to provide a better understanding of how to mitigate cybercrime through effective change, it is important to rely on data regarding the visibility of cyber victimization and the effect of the conditions when considering the motivated offender and how to create an atmosphere to curb that motivation (Choi et al., 2016). One of the understood factors of criminology is the theory that crime will consist of three factors: motivation, opportunity, and the lack of a capable guardian. These factors can apply in an individual incident as well as established trends.

Derived originally to explain physical crimes, it is equally applicable across cyberspace (Grabosky, 2001). Through understanding the crime triangle and applying methods that can be utilized by cybersecurity analysts, the implementation of this methodology can provide the impetus for new strategies that would create an added layer of protection against external cyber security threats.

Subtheme: Analyst's Views of Cybersecurity Strategy

Cybersecurity analysts are an asset to any cybersecurity policy or procedure as they help set the tone for the organization's security policy and threat assessment. Cybersecurity analysts make decisions based on facts and data gathered from within the organization. Cybersecurity analysts spend countless hours assessing threats, investigating anomalies, and testing new tools. The viewpoint of cybersecurity analysts is an essential aspect of how their expertise is received within the organization. Each participant discussed the importance of cybersecurity and how they viewed aspects of the cybersecurity strategy followed by the organization. Participants 1, 3, 4, 5, 6, 8, and 9 were very responsive and provided information deemed as firmly held positions on the security practices held by their organizations. P1 explained that they think their company does cybersecurity very efficiently and it is very agile. Being agile is huge as it provides benefits such as being mobile and being ready for change. It also provides an arena where things can be tested without going through excessive processes. P3 touted that cybersecurity is tough as you must stay on top of everything. P3 also explained that many younger employees spend time digging into threats even when not on the clock. P3 stated, "I am no longer at that point in my career." P4 provided insight into the hiring process, the importance of hiring experienced personnel, and the risks associated with hiring inexperienced personnel that leads to a lack of proper documentation and inefficient processes for engineers, developers, and incident response groups. P5 explained that the current organization lacks many processes and procedures, and the security apparatuses were not built to handle the amount of data that pertains to threats. P5 further stated, "It is one of the scariest places I have ever worked.” P6 explained that it is vital to distinguish between opportunistic attacks and targeted attacks. Opportunistic attacks are mostly automated of low complexity and seek to penetrate nonvulnerable conditions within a network and its configurations. P6 further opined that the most important thing within the organization is dealing with the people and the culture within the organization. A general understanding of the people and culture within the organization means that everyone must play an active role in protecting the organization, as it is essential to monitor the level of preparedness and prevention within the organization. P8 opined that the organization is more afraid of auditors than the actual adversary. P8 further elaborated that he preferred a more defensive approach to security. P8 stated, “It’s like a cat and mouse game. What I like to tell my customers, we prevent hackers from penetrating their assets, and the best way to do that is to make things a bit more inconvenient by staying one step ahead of the hacker. It’s kind of our focus to be ahead of the hackers” P9 explained that the most effective strategies consist of not just one control but a combination of things. P9 also stated,

> There is no silver bullet, to be honest. It is an aggregation of using different standards and, most importantly, continuous monitoring. … Just understand no

> matter what standard you use, it is important to look at the assessment through different lenses and understand where the gaps are. So, it’s more a combination of multiple things and mainly because different workloads will require different levels of assessment.

NIST documentation does not outline the viewpoints of cybersecurity analysts as a defense-in-depth strategy in support of this theme; however, cybersecurity analysts play an important role in providing cybersecurity for a small business as well as in providing novel and innovative practices, based on their experiences and application of technologies, which allows small business to compete with their larger counterparts in protecting their organizations. Additionally, how a cybersecurity analyst views the cybersecurity strategy that has been instituted by the organization, the understanding of the organizational culture is equally as essential in understanding and defining the security culture (Wiley et al., 2020). Establishing a successful cybersecurity network that handles threats efficiently, the ability to identify and support essential cybersecurity behaviors, as well as the ability to align security and awareness activities with internal and external strategies are essential to improving the cybersecurity culture (Alshaikh, 2020).

When reviewing the literature, cybersecurity analysts are indispensable when it comes to assessing the organization and applying a cybersecurity strategy that protects the most critical assets within the organization. As Von Solms and Von Solms (2018) articulated, the meaning of the term cybersecurity translates to protecting data from unauthorized access or attacks fitted for exploitation. Cybersecurity analysts adopt strategies that best fit the business goals of the organization as this provides the clearest path to adequately defending their organizations. When navigating a small business, there are several concerns when outlining a cybersecurity strategy and addressing policy initiatives. There are three main areas of concern when applying a finite set of resources: staffing, financial, and resource deficits (Selznick & LaMacchia, 2018). Cybersecurity analysts create innovative strategies based on the business needs of their organization, as often times budget concerns are a limitation that can control varying aspects of how assets are protected and maintained. Small businesses must strike a delicate balance between integrating new internet-based technologies to remain competitive and formulating a cybersecurity strategy that can effectively secure and maintain those systems (Berry & Berry, 2018). Cybersecurity analysts' viewpoints are highly regarded when preparing to establish a cybersecurity strategy that will protect critical assets within a small business network. C-level buy-in is chiefly established from data provided by cybersecurity analysts and their ability to relay their vision for cybersecurity to protect the organization. Ultimately, the direction of the cybersecurity strategy rests in the hands of the C-level executives. Bauer and Bernroider (2017) noted that senior-level executives play the most significant role in supporting the development and implementation of the cybersecurity program and its strategic purpose, which encapsulates policies and procedures created to protect organizational communications, assets, and systems from external as well as internal cybersecurity threats.

The concepts of RAT are inextricably tied to all aspects of the cybersecurity strategy. Cohen and Felson's (1979) RAT is leveraged in this study to explore issues that provide the impetus for cybercrime activities referencing an offender, a suitable target, and the absence of a control or mitigation technique. The cybersecurity strategy formulated by cybersecurity analysts entails creating conditions that foster a capable guardian, which can be translated into the implementation of improved or innovative cybersecurity controls, personnel, or policies. When reviewing the research, the researcher's goal was to provide data that would measure the effectiveness of a more capable guardian while reducing the suitability of the targets to prevent, intervene, and respond to incidents (Choi et al., 2018). The concepts of RAT also entail the existence of a suitable target. Cybersecurity analysts can affect this aspect by providing new and innovative ways, as outlined in this study, to create a communication network that informs surrounding small businesses of threats and their tips, tactics, and procedures, thereby creating conditions that would foster a less suitable target. Fostering the creation of a less suitable target may prove to add a layered prevention strategy, whether those actions pertain to the environmental, spatial, or absence of any of the three required elements for a crime to be committed (Choi et al., 2018).

The concept of RAT also entails the aspect of a motivated offender, the least likely aspect whereby cybersecurity analysts can effect change; this aspect can be achieved by providing a more layered defense in depth strategy that would, in theory, foster conditions that would lead to the offender becoming less likely motivated to attack the organization due to the target's lessened suitability and causing the offender to yet chose another target. Considering the spatial elements as it applies to RAT, which consists of time, space, and the motivated offender's perception of an ideal target, it is vital to understand how to reduce the risk of victimization. By applying RAT principles, IT cybersecurity analysts may have adequate leverage in contributing to reducing the risks associated with victimization-related events (Choi et al., 2016). The concepts of RAT can also be affected by other innovative strategies mentioned in this study, such as varying the routine activities of the targets and capable guardians, moving target defenses, as well as spatial components that deal with the accessibility of the systems as a new strategy. These methodologies and strategies bare some insight into thinking outside of the box and utilize a strategy that accounts for time, location, the motivated offender, and suitable target methodologies for identified threats that provide notable relatability to a newly formulated strategy in this study according to the concepts of RAT utilizing proximity and time as a strategy for data protection against external threats (Wen-qun, 2006). Furthermore, such innovations could lead to the initiation of a pragmatic approach and the procedural enhancement of the organization's cybersecurity policy in protecting critical data assets and information systems (Baldwin et al., 2017).

Applications to Professional Practice

The strategies outlined in this study's findings, which consist of the literature review as well as a comprehensive analysis of the conceptual framework, highlight a set of innovative methods that can be leveraged in the prevention of external cybersecurity threats perpetrated against small businesses. The results of this study provided a perspective that analyzes strategies for the protection of critical infrastructures while leveraging a physical crime theory in a virtual environment. These concepts of security controls are instrumental in providing security measures that are innovative and can help improve strategies in the prevention of data breaches. When combining knowledge of traditional cybersecurity controls, coupled with mitigation techniques of cybercrime which add greater obscurity to a system hindering the external attacker's ability to gain knowledge within a network, geospatial techniques, MTD, and time-varying dynamic models, may aid in threat mitigation or external cybersecurity threats when translated to cybercrime, improving the efficacy of defense in depth strategies and providing findings that can advance a higher level of administrative policies to reduce external cybersecurity threats.

The outcomes derived from this study illuminate the need for small businesses with susceptibility to external cybersecurity threats to provide new and innovative defense-in-depth strategies in the protections of their critical infrastructure networks. Leveraging the conceptual framework of RAT, which includes all three aspects of the framework (effecting the motivations of the offender, enhancing the capabilities of the guardian, creating conditions to make the target less suitable) as a basis for the control model, as well as the implementation of the newly formulated strategy which includes a person, process, or technology cybersecurity analysts are better equipped to provided additional layers of defense within the set of an organizations' cybersecurity controls thereby strengthening the entire security posture of the organization. Utilizing these methods as a cornerstone when applying security controls across the organization enhances the security of the control itself. In order to provide more effective strategies in regards to preventing threats from materializing, which includes a motivated offender, the defense-in-depth strategies, along with considering the framework of RAT, should include but are not limited to (a) MTDs (b) geospatial techniques, (c) varying routine activities of personnel, (c) time-varying dynamic models, (d) behavioral analytics, (e) risk analysis utilizing TTPs, (f) intelligence-based mitigation, (g) a layered defense strictly based on innovation, as well as (h) a comprehensive understanding of the business goals.

Applying these innovative strategies in conjunction with viable cybersecurity concepts that are cost-effective allows small businesses to compete with their larger counterparts in finding affordable strategies that are proven to aid in the mitigation of external cybersecurity threats. The strategies outlined in this study's findings align with the conceptual framework of RAT as it provides an applicable framework conducive to defensive strategies that positively affect the motivations of an offender and enhance the capability of a guardian while decreasing the suitability of a target.

Implications for Social Change

The outcomes outlined in this study's findings indicate that positive social change can be obtained by utilizing small business strategies to prevent external cybersecurity threats in defending their critical infrastructures while mitigating exposure to customer PII. By providing small business cybersecurity analysts with additional strategies to effectively mitigate cybersecurity threats, these findings may lead to more effective protection of PII and financial stability for small businesses, creating more significant economic growth in local communities. Small businesses are amongst the most targeted critical infrastructures in the United States. Data breaches pose an enormous concern on the viability of the critical infrastructures that make up the lion's share of jobs in North America. Small businesses are a key part of the economic system, and data breaches threaten the viability of these organizations. Providing a more secure critical infrastructure for small businesses ensures greater economic stability for the organization, thereby creating greater economic stability amongst the community, as small businesses are the number one providers of jobs in the country.

As outlined in this study, small businesses should apply strategies that allow them to explore innovative methods for the protection of their critical infrastructures. Adopting a proactive defense-in-depth methodology that rewards innovation may lead to enhanced protection of customer PII and national economic security. Positive social change implications include sharing innovative and effective small businesses' cybersecurity strategies with like critical infrastructures. The benefits to the community would include a more secure economic job market with continued growth and reduction in the compromise of customer PII decreasing the compromise of personally identifiable, confidential, or sensitive customer information. More so, enhancing cybersecurity strategies in small business organizations may provide a better allocation of finite resources to aid in formulating new techniques and strategies that enhance the prevention of customer PII while delivering even greater economic job stability amongst communities.

Recommendations for Action

This pragmatic qualitative inquiry is intended to explore small business cybersecurity analysts' strategies to prevent external cybersecurity threats. This study analyzed industry standards utilized by organizations participating in the study, semistructured interview responses from accomplished cybersecurity analysts, multiple scholarly literature research documents, and cybersecurity strategies leveraged by the participants in the study. These four types of data supported triangulation and corroboration of the research question. Based on this triangulation of the data, six themes emerged: (a) applying standards regarding external threats, (b) consistent evaluation of cybersecurity strategies and effectiveness, (c) consistent awareness of the external threat landscape, (d) assessing threat security posture, (e) measuring the ability to address risk and prevent attacks related to external threats, (f) centralizing communication across departments to provide perspective on threats.

The outcomes outlined in this study's findings provide insight into key small business cybersecurity strategies that cybersecurity analysts utilize in the prevention of external cybersecurity threats. The small businesses' cybersecurity strategies utilized in the prevention of external cybersecurity threats must be addressed by cybersecurity analysts, as the cost of a single data breach can leave a small business inoperable. Therefore, providing new and innovative strategies that are cost-effective can further enhance the viability of small businesses. These strategies that are effective from this study for cybersecurity analysts consist of the following:

- MTDs
- geospatial techniques
- varying routine activities of personnel
- time-varying dynamic models
- behavioral analytics
- risk analysis utilizing TTPs

- mitigation-based intelligence (AI)
- layered defense strictly based on innovation
- comprehensive understanding of the business goals

Policies, procedures, and industry standards that govern each cybersecurity strategy and how it is leveraged and utilized within an organization can pose challenges within an organization as outlined in the subtheme of this study (challenges in implementing industry standards). Based on the findings of this study, it is recommended that cybersecurity analysts consider the concepts of RAT that seek to mitigate or omit one of the three aspects of the crime triangle in conjunction with any implemented strategy or control, thereby creating conditions that enhance the security posture of the organization. The findings from the study validate the claims form the literature, as participants were not aware of such strategies as provided in this study. By adhering to the findings in this study, cybersecurity analysts can effectively implement new controls that leverage industry standards based on a comprehensive understanding of the business goals in conjunction with new and innovative strategies, as represented in this study.

Small businesses are considered soft targets and therefore are the most targeted. Cybersecurity analysts can leverage data from this study that outlines varying the routine activities of personnel to add another layer of defense within their organization that is cost-effective. Small businesses do not possess the resources of their larger counterparts and require more attention to innovation as well as conducting a more precise risk analysis. By leveraging the findings from this study, cybersecurity analysts can implement additional layered defense strategies that are cost-effective and provide more comprehensive security controls based on concepts and innovation. I would also recommend that organizations build a tightly knit communication system where data on threats can be shared within the small business community to keep them appraised of the tips, tactics, and procedures of the latest threats and social engineering tactics that exist.

After receiving CAO approval, the results of the study shall be disseminated among each of the nine research participants. I shall also publish this study in ProQuest, where the information can be reviewed and leveraged to further other research or provide an impetus for greater inquiry into some of the concepts provided in this study. Finally, I will seek to share this information with the academic community in forums such as workshops, journals, publications, conferences, and seminars.

Recommendations for Further Study

The findings of this study provided an analysis of small business strategies to prevent external cybersecurity threats leveraged by cybersecurity analysts. The limitations of the study can be addressed by future researchers reviewing this study to compare any salient themes that are consistently based on the data gathered in the study to validate that the data informed each study as opposed to each researcher's experiences. Addressing the limitation of sensitive information being shared about cybersecurity strategies from each organization is an inherent part of this study and may be an aspect of this topic that may not be overcome. However, a slight alteration in the subject matter and how it is approached may provide some insight into an organization being more forthcoming. In addressing the last limitation, researchers may seek organizations that employ research participants who execute threat management and threat prevention in a singular position to further inform cybersecurity analysts in the prevention of small business external cybersecurity threats.

This study leveraged the concepts of RAT that consisted of analyzing aspects of the crime triangle as it translates from a physical crime to a virtual crime. Certain attributes of the crime must exist for the commission of the crime to take place. This consisted of the motivations of the offender, the capability of the guardian, and the suitability of the target. More research is needed in the areas that leverage the effect of outside stimuli (mitigating controls, polices, procedures) would have on the motivations of an offender as it widely varies. This area of study is focused on the attacker and what are some of the factors that would curb their motivations based on the target's suitability and its value to the attacker. Providing further research that probes the physical crime triangle and how it compares and contrasts in consideration of security controls within a virtual crime setting as well as how these concepts can be applied to build stronger security controls, can help to formulate more efficient security models within an organization. When applying new perspectives that leverage the three attributes of the crime triangle, newly formed strategies may emerge. Analyzing the ways it affects the security posture of an organization coupled with people, processes, and technology that are utilized within the security policies and procedures of an organization could prove to create a new set of protocols that can be leveraged by small businesses. I would also recommend expanding the geographic location as small businesses are across all 50 states and require more studies attributed to different sectors of small business to gain a comprehensive understanding of the phenomena and their soft target perceptions.

Reflections

This academic journey of completing my DIT Doctoral Study has been one of the most challenging endeavors I have ever experienced in my life. With the advent of work, family, death, and COVID staying motivated was a key factor in getting to the finish line. This was a harrowing experience, to say the least, and it was a dream of mine for a long time to complete my doctoral degree. I will be the first in my family to achieve this feat. I must admit there were many obstacles; however, I wouldn't change a thing as it makes the academic journey even more satisfying. Possessing over 35 years of experience in the field help provide a perspective on the degree that helps me to understand the dedication it takes to achieve a feat such as this.

As an IT professional who has held many positions in the field, I came in without any preconceived notions and checked my ego and biases at the door to receive the full measure the doctoral program had to offer. I believe this helped me to follow the research and allowed it to guide me along the path of understanding the methodology of properly researching a new phenomenon in my field of practice. The doctoral process and all its many levels of inquiry, research, and triangulation provided me with another level of respect for the process as well as the academic journey. I would say that this process is not for the faint of heart, as it is everything it has been billed to be.

Summary and Study Conclusions

Analyzing strategies small businesses utilize to prevent cybersecurity threats is not only an essential aspect of the economic health of small businesses, but it also translates into providing economic stability for the nation, as small businesses are the number one supplier of jobs in the country. A breakdown in this area caused by data breaches could be detrimental to the economic sector's survival and stability. The purpose of this pragmatic qualitative inquiry was to explore strategies that cybersecurity analysts utilized in the prevention of external cybersecurity threats and to provide alternative and enhanced strategies that are cost-effective, and that would be key in providing additional layered defenses to curb threats. The specific problem is that some IT cybersecurity analysts of small businesses lack the strategies to prevent external cybersecurity threats. This pragmatic qualitative inquiry investigated cybersecurity strategies utilized by cybersecurity analysts in the prevention of small business external cybersecurity threats. The study answered the research question: What strategies do cybersecurity analysts of small businesses use to protect their systems from external cybersecurity threats? Nine cybersecurity analysts from six small business organizations in Texas participated in semistructured interviews. This study indicated that the following are security strategies that cybersecurity analysts seldom use. However, this study highlights these methods as controls that can provide an additional level of defense in depth, helping to better secure small businesses networks:

- MTDs
- geospatial techniques
- varying routine activities of personnel
- time-varying dynamic models
- behavioral analytics
- risk analysis utilizing TTPs

- mitigation-based intelligence (AI)
- layered defense strictly based on innovation
- comprehensive understanding of the business goals

These mitigation techniques can provide innovative strategies to equip cybersecurity analysts with defense-in-depth concepts to further improve the security posture of their organizations and protect customer-sensitive data. Griffioen et al. (2021) proposed that if the connection is made between the division of cybercrime and physical crime, as well as innovative internal applications that can be framed based on these factors, it could lead to positive change that efficiently mitigates cybercrime. Further development of these concepts may be achieved by adding greater obscurity to a system, hindering the external attacker's ability to gain knowledge within a network. Applying these new and innovative methodologies can enhance defense-in-depth strategies that may provide a more secure network decreasing the risk of compromising customer-sensitive data while strengthening local communities.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulations as a methodological alternative. *Administração: Ensino e Pesquisa*, *19*(1), 66-98. https://doi.org/10.13058/raep.2018.v19n1.578

Adams, C., & van Manen, M. A. (2017). Teaching phenomenological research and writing. *Qualitative Health Research*, *27*(6), 780-791. https://doi.org/10.1177/1049732317698960

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

Alase, A. (2017). The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, *5*(2), 9-19. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Ali, M., Bilal, K., Khan, S. U., Veeravalli, B., Li, K., & Zomaya, A. (2018). DROPS: Division and replication of data in the cloud for optimal performance and security. *IEEE Transactions on Cloud Computing*, *6*(2), 303-315. https://doi:10.1109/TCC.2015.2400460

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

Almutairi, M., & Riddle, S. (2018). *A framework for managing security risks of* *outsourced IT projects: An empirical study* [Paper presentation]. Proceedings of the 2018 International Conference on Software Engineering and Information Management, Casablanca, Morocco. https://doi.org/10.1145/3178461.3178476

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, Article 102003. https://doi.org/10.1016/j.cose.2020.102003

Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a codebook. *Comprehensive Psychology*, *3*(4), 1–7. https://doi.org/10.2466/03.CP.3.4

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). An introduction to data analysis for auditors and accountants. *CPA Journal*, *87*(2), 32-37.

Association of Computing Machinery Joint Task Force on Cybersecurity Education. (2016). ACM Joint Task Force on Cybersecurity Education. https://www.semanticscholar.org/paper/Towards-a-Contemporary-Definition-of-Cybersecurity-Schiliro/b1508de4869d54579b532454eb10ddcac0cfbc94

Au, M. H., Liang, K., Liu, J. K., Lu, R., & Ning, J. (2018). Privacy-preserving personal data operation on mobile cloud-chances and challenges over advanced persistent threat. *Future Generation Computer Systems*, *79*, 337-349. https://doi.org/10.1016/j.future.2017.06.021

Ayereby, M. P.-M. (2018). Overcoming data breaches and human factors in minimizing threats to cyber-security ecosystems (Doctoral Dissertation).

Bace, R., & Mell, P. (2000*). Intrusion detection systems* (Report no. 800-31). U.S.

Department of Commerce, National Institute of Standards and Technology. https://www.nist.gov/publications/intrusion-detection-systems

Bada, M., & Nurse, J. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 1-20. https://doi.org/10.1108/ICS-07-2018-0080

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

Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces, 54*, 176-185. https://doi.org/10.1016/j.csi.2016.11.010

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

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database, 48*(3), 44–68. https://doi.org/10.1145/3130515.3130519

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

Bell, S. (2017). Cybersecurity is not just a 'big business' issue. *Governance Directions*, *69*, 536-539. https://www.governanceinstitute.com.au/media/881982/cybersecurity-sme-october-2017.pdf

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8-14. https://doi.org/10.1016/j.npls.2016.01.001

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

Berry, C. T., & Berry, R. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 9. https://doi.org/10.1504/ijbcrm.2018.090580

Brantingham, P. J., & Brantingham, P. L. (Eds.). (1981). *Environmental criminology*. Sage Publications.

Bromiley, M. (2019). *Thinking like a hunter: Implementing a threat hunting program* [White paper]. https://www.sans.org/reading-room/whitepapers/analyst/thinkinghunter-implementing-threat-hunting-program-38923

Brown, A., & Danaher, P. A. (2019). CHE Principles: facilitating authentic and dialogical semistructured interviews in educational research. *International Journal of Research & Method in Education*, *42*(1), 76-90. https://doi.org/10.1080/1743727X.2017.1379987

Bryan, L. L. (2020). Effective information security strategies for small business. *International Journal of Cyber Criminology*, *14*(1), 341-360. https://doi.org/10.5281/zenodo.3760328

Buch, R., Ganda, D., & Kalola, P. (2017). World of cyber security and cybercrime. *Recent Trends in Programming Languages*, *4*(2), 18–23.

Budzak, D. (2016). Information security: The people issue. *Business Information Review*, *33*(2), 85-89. https://doi.org/10.1177/0266382116650792

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548. https://doi.org/10.2307/25750690

Bunch, J., Clay-Warner, J., & Lei, M. (2015). Demographic characteristics and victimization risk: Testing the mediating effects of routine activities. *Crime & Delinquency*, *61*(9), 1181-1205. https://doi.org/10.1177/0011128712466932

Burley, D. (2017). *The United States House of Representatives Committee on Science, Space & Technology Subcommittee on Research and Technology, hearing on, Strengthening U.S. Cybersecurity Capabilities*, 115th Cong. (2017) (testimony of Dr. Charles H. Romine). https://republicans-science.house.gov/2017/2//research-and-technology-subcommittee-hearing-strengthening-us-cybersecurity

Caldamone, A. A., & Cooper, C. S. (2017). The institutional review board. *Journal of Pediatric Urology*, *13*(6), 557-558. https://doi.org/10.1016/j.jpurol.2017.10.006

Calvard, T. S., & Jeske, D. (2018). Developing human resource data risk management in the age of big data. *International Journal of Information Management*, 43, 159-164. https://doi.org/10.1016/j.ijinfomgt.2018.07.011

Cameron, C., & Kornhauser, L. (2015). Rational choice attitudinalism? *European Journal of Law and Economics, 43*(3). https://doi.org/10.1007/s10657-015-9512-1

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

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

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811-830. https://doi.org/10.46743/2160-3715/2016.2337

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

Chen, Q. (2019). Toward realizing self-protecting healthcare information systems: Design and security challenges. *Advances in Computer Science*, *114*(2), 113-149. https://doi.org/10.1016/bs.adcom.2019.02.003

Chen, M., Herrera, F., & Hwang, K. (2018). Cognitive computing: Human-centered computing with intelligence on clouds. *IEEE Access*, *99*, 19774-19783. https://doi.org/10.1109/ACCESS.2018.2791469

Cheng, Z., Cui, B., Qi, T., Yang, W., & Fu, J. (2021). An improved feature extraction approach for web anomaly detection based on semantic structure. *Security and Communication Networks*, *2021*, Article 6661124. https://doi.org/10.1155/2021/6661124

Choi, K., Earl, K., Lee, J., & Cho, S. (2018). Diagnosis of cyber and non-physical bullying victimization: A lifestyles and routine activities theory approach to constructing effective preventative measures. *Computers in Human Behavior*, *92*, 11-19. https://doi.org/10.1016/j.chb.2018.10.014

Choi, K., & Lee, J. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402. https://doi.org/10.1016/j.chb.2017.03.061

Choi, K., Cronin, S., & Correia, H. (2016). The assessment of capable guardianship measures against bullying victimization in the school environment. *Police Practice and Research*, *17*(2), 149-159. https://doi.org/10.1080/15614263.2015.1128161

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

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

Clarke, R. V., & Eck, J. (2003). *Become a problem-solving crime analyst: In 55 small steps*. London: Jill Dando Institute of Crime Science. Adapted from *Oxford Research Encyclopedia, Criminology and Criminal Justice* https://oxfordre.com/criminology

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: does size matter?. *Journal of Advanced Nursing, 70,* 473-475. https://doi.org/10.1111/jan.12163

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://www.asanet.org

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review*, *46*(5), 505.https://doi.org/10.2307/2094935

Cook, M. (2017, June 26). Cybersecurity growing concern: Online attacks spur corporate measures to defend the wall. *Arkansas Business*, *34*(26), 9. https://www.arkansasbusiness.com/article/117565/online-attacks-spur-corporatecybersecurity-measures-to-defend-the-wall

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

Congressional Research Service. (2014). Cybersecurity Issues and Challenges: In Brief. (R43831). https://www.fas.org/sgp/crs/misc/R43831.pdf

Cornish, D., & Clarke, R. (1986). The reasoning criminal: Rational choice perspectives on offending.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *25*(4), 933–947. https://doi.org/10.1111/j.1745-9125.1987.tb00826.x

Cornish, D. B., & Clarke, R. V. (2008). The rational choice perspective: Environmental criminology and crime analysis. Willan Publishing.

Cozzolino, A., Verona, G., & Rothaermel, F. T. (2018). Unpacking the disruption process: New technology, business models, and incumbent adaption. *Journal of Management Studies*, *55*, 1166-1202. https://doi.org/10.1111/joms.12352

Cunningham, P., & Head, S. (2019). Cybersecurity readiness as a business value. *The RMA Journal*, *101*(5). https://www.rmahq.org/cybersecurity-readiness-as-abusiness-value

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing*, *36*(4), 253-263. https://doi.org/1097/DCC.0000000000000253

D'Arcy, L., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information System Journal*, *29*, 43-69. https://doi.org/10.1111/isj.12173

Dawson, M., Dawson, M., Eltayeb, M., & Omar, M. (2016). Security Solutions for Hyperconnectivity and the Internet of Things. IGI Global

Denscombe, M. (2013). The role of research proposals in business and management education. *The International Journal of Management Education*, *11*(3), 142–149. https://doi.org/10.1016/j.ijme.2013.03.001

Department of Homeland Security. (2019). (*Critical Infrastructure Sectors | CISA*, n.d.) https://www.cisa.gov/critical-infrastructure-sectors

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, *56*, 63-69.

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic Insurance). *The Qualitative Report*, *21*(3), 10. https://doi.org/10.46743/2160-3715/2016.2243

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

Doneda, D., & Almeida, V. (2015). Privacy governance in cyberspace. *IEEE Internet Computing*, *19*(3), 50-53.

Draper, J. (2015). Ethnography: Principles, practice, and potential. *Nursing Standard*, *29*(36), 36-41. https://doi.org/10.7748/ns.29.36.36.e8937

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. In M. J. Smith & D. B. Cornish (Eds.), Crime prevention studies 16(1), 7-39. Monsey, NY: Criminal Justice Press. https://www.researchgate.net/profile/John-Eck/publication/258440181_Classifying_Common_Police_Problems_A_Routine

_Activity_Theory_Approach

Edwards-Jones, A. (2014). Qualitative data analysis with NVivo 12 SOFTWARE. *Journal of Education for Teaching*, *40*(2), 193–195. https://doi.org/1080/02607476.2013.866724

Eisenhauer, E. R., Tait, A. R., Rieh, S. Y., & Arslanian-Engoren, C. M. (2019). Participants' understanding of informed consent for biobanking: A systematic review. *Clinical Nursing Research*, *28*(1), 30-51. https://doi.org/10.1177/1054773817722690

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491-497. https://doi.org/10.1016/j.jare.2014.02.006

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *Sage Open*, *4*(1), 1-10. https://doi.org/10.1177/2158244014522633

Ene, P. (2019). Cyber Security the Great Challenge of the 21St Century. *Romanian Military Thinking*, *4*, 136–149.

Farber, D. M, (2018). GAO Reports Challenges and Successes in Cybersecurity Framework Adoption. The Power of Collaboration. *Van Ness Feldman LLP.* https://www.vnf.com/gao-reports-challenges-and-successes-in-cybersecurity-framework

Fellnhofer, K. (2018). Game-based entrepreneurship education: impact on attitudes, behaviors, and intentions. *World Review of Entrepreneurship, Management and*

Sustainable Development, *14*, 205-228. https://doi.org/10.1504/WREMSD.2018.089066

Felson, M., & Eckert, M. (2019). Crime and everyday life: A brief introduction (Sixth Edition). SAGE Publications.

Federal Emergency Management Agency. (2018). *Be prepared for a cyberattack*. https://www.fema.gov

Federal Trade Commission. (2022). *Understanding the NIST cybersecurity framework*. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

Fink, A. S. (2000). The role of the researcher in the qualitative research process. A potential barrier to archiving qualitative data. *Forum: Qualitative Social Research*, *1*(3), 16. https://doi.org/10.17169/fqs-1.3.1021

Forde, E. S. (2017). Security strategies for hosting sensitive information in the commercial cloud (Doctoral Dissertation).

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigor of qualitative research in emergency medicine. *BMC Health Services Research*, *18*(1). https://doi.org/10.1186/s12913-018-2915-2

Freitas, F., Ribeiro, J., Brandão, C., de Almeida, C. A., & de Souza, F. N. (2019). How do we like to learn qualitative data analysis software? *The Qualitative Report*, *24*(13), 21. https://doi.org/10.46743/2160-3715/2019.4133

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development, 91*, 184-194. https://doi.org/1002/j.1556-6676.2013.00085.x

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20,* 1408-1416. https://doi.org/10.46743/2160-3715/2015.2281

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM*), *7*(1), 14-26.]

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report, 20*(11), 1772-1789. https://pdfs.semanticscholar.org

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

George, R., Truong, T., & Davidson, J. (2017). Establishing an effective data governance system. *Pharmaceutical Technology Europe, 29*(11), 40-43.

Ghourab, E., Azab, M., & Mansour, A. (2019). Spatiotemporal diversification by moving-target defense through benign employment of false-data injection for dynamic, secure cognitive radio network. *Journal of Network and Computer Applications, 138*, 1-14. https://doi.org/10.1016/j.jnca.2019.02.020

Gill, M. J. (2014). The possibilities of phenomenology for organizational research. *Organizational Research Methods, 17*(2), 118–137. https://doi.org/10.1177/1094428113518348

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods, 16*, 15-31. https://doi.org/1177/1094428112452151

Gong, S., & Lee, C. (2021). Threat intelligence framework for incident response in an energy cloud platform. Electronics, 10, 1–19. https://doi.org/10.3390/electronics10030239

Goode, J. (2018). Comparing training methodologies on employee's cybersecurity countermeasures awareness and skills in traditional vs. socio-technical programs (Doctoral Dissertation).

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

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005, Oxford Academy. https://doi.org/10.1093/cybsec/tyaa005

Grabosky, P. (2001). "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies 10*(2):243–249.

Grace, K., Vincent, M., & Evans, A. (2018). Corporate governance and performance of financial institutions in Kenya. *Academy of Strategic Management Journal*, *17*(1), 1-13. http://www.abacademies.org/journals/academy-of-strategicmanagement-journal-home.html

Graebner, M. E., Martin, J. A., & Roundy, P. T. (2012). Qualitative data: Cooking without a recipe. *Strategic Organization*, *10*(3), 276–284. https://doi.org/10.1177/1476127012452821

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

Griffioen, P., Weerakkody, S., & Sinopoli, B. (2021). A Moving Target Defense for Securing Cyber-Physical Systems. *IEEE Transactions on Automatic Control*, *66*(5), 2016–2031. https://doi.org/10.1109/TAC.2020.3005686

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

Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and computation: Practice and experience*, *32*(21), e4946. https://doi.org/10.1002/cpe.4946

Gwebu, K. L., Jing, W., & Li, W. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information*, *35*(2), 683-714. https://doi.org/10.1080/07421222.2018.1451962

Hagen, J., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information and Computer Security*, *17*(5), 388-407.

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

Han, W., Xue, J., Wang, Y., Zhang, F., & Gao, X. (2021). APTMalInsight: Identify and cognize APT malware based on system call information and ontology knowledge framework. *Information Science,* 546(2021), 633–644. https://doi.org/10.1016/j.ins.2020.08.095

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

Hawdon, J., Costello, M., Ratliff, T., Hall, L., & Middleton, J. (2017) Conflict Management Styles and Cybervictimization: Extending Routine Activity Theory, *Sociological Spectrum*, *37*(4), 250-266. https://doi.org/10.1080/02732173.2017.1334608

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amide COVID19: the initial results from a natural experiment. *American Journal of Criminal Justice*, 45, 546–562. https://doi.org/10.1007/s12103-020-09534-4

Hawley, A., H. (1944). Ecology and human ecology. *Social forces*, 398-405.

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

Henson, B., Reyns, B. W., & Fisher, B. S. (2016). Cybercrime victimization. In C.Cuevas & C. M. Rennison (Eds.), The Wiley Handbook on the Psychology of Violence (pp. 555-569). John Wiley & Sons, Ltd.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization. Cambridge, MA: Ballinger.

Hintze, M. (2018). Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the GDPR. *Journal of Law Technology & the Internet*, *22*(2), 17-31. https://doi.org/10.2139/ssrn.3192721

Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organizational response to regulative pressure in information security management: The case of a Chinese hospital. *Technological Forecasting and Social Change, 126*, 64-75. https://doi.org/10.1016/j.techfore.2017.03.023

Humaidi, N., & Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behavior towards information security policies. *Health Information Management Journal*, *47*, 17-27. https://doi.org/10.1177/1833358317700255

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*(1), 2-18.

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

Internet Crime Complaint Center. (2018a). Federal Bureau of Investigations. 'Internet

Crime Complaint Center, http://www.ic3.gov

Internet Crime Complaint Center. (2018b). Internet Crime Report (pp. 1–28). 'Federal Bureau of Investigation', https://pdf.ic3.gov/2018_IC3Report.pdf

Internet Crime Report. (2021). Federal Bureau of Investigations. 'Internet Crime Complaint Center', *The National Cyber Investigative Joint Task Force Ransomware fact sheet*. https://www.fbi.gov/news/pressrel/press-releases/the-national-cyber-investigative-joint-task-force-releases-ransomware-fact-sheet

(ISC)2. (2020). CISSP-Certified information systems security professional. Retrieved from https://www.isc2.org/Certifications/CISSP

Iverson, A., & Terry, P. (2018). PLAN AUDITS: Cybersecurity Hot Topics for Closely-Held Businesses. *Journal of Pension Benefits, 25*(4), 60–62. http://search.proquest.com/central/docview/2085803232/abstract/7A273D080B394679PQ/1

Jackson, R. (2018). Pulling strings. Internal Auditor, 75(4), 34 – 39. Business Source Premier.

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

Jasinki, J., & Navarro, J. (2012). "Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences." *Sociological Spectrum.32*(1), 81-94

Jeffery, C. R. (1971). Crime Prevention Through Environmental Design. SAGE Publications.

Jensen, M., Dinger, R., Wright, L., & Thatcher, J. (2017). Training to Mitigate Phishing

Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, *34*(2), 597-626. https://doi.org/10.1080/07421222.2017.1334499

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, *33*(7), 14-26. https://doi.org/10.3102/0013189X033007014

Joshi, A., Bollen, L., Hassink, H., DeHaes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information & Management*, *55*(3), 368-380.

Kabalci, Y. (2019). 5g mobile communication systems: Fundamentals, challenges, and key technologies. Smart Grids and Their Communication Systems (pp. 329-359). Springer, Singapore.

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.ezp.waldenulibrary.org/10.1080/10919392.2018.1484598

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

Kakucha, W., & Buya, I. (2018). Information system security mechanisms in financial management. *Journal of Information Science and Technology*, *2*(1), 1-16. https://stratfordjournals.org

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information and Computer Security*, *25*, 300-329. https://doi.org/10.1108/ics02-2026-0013

Karlsson, F., Karlsson, M., & Åström, J. (2017). Measuring employees' compliance – the importance of value pluralism. *Information and Computer Security*, *25*(3), 279-299.

Kassan, A., Goopy, S., Green, A., Arthur, N., Nutter, S., Russell-Mayhew, S., Vazquez, M., & Silversides, H. (2018). Becoming new together: Making meaning with newcomers through an arts-based ethnographic research design. *Qualitative Research in Psychology*, 1-18. https://doi.org/10.1080/14780887.2018.1442769

Kaukola, J., Ruohonen, J., Tuomisto, A., Hyrynsalmi, S., & Leppänen, V. (2017). Tightroping between APT and BCI in small enterprises. *Information & Computer Security*, *25*, 226-239. https://doi.org/10.1108/ICS-07-2016-0047

Khan, K., & Goodridge, W. (2019). A survey of network-based security attacks. *International Journal of Networking*, *10*, 3981-3989. https://doi.org/10.35444/IJANA.2019.10051

Khan, S. N. (2014). Qualitative research method: Grounded theory. *International Journal of Business & Management*, *9*(11), 224–233. https://doi.org/10.5539/ijbm.v9n11p22

Khey, D., & Sainato, V. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal*, *26*, 367–382. https://doi-org.ezp.waldenulibrary.org/10.1057/sj.2013.244

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470–486. https://doi.org/10.1177/0894439311422689

Kihn, L., & Ihantola, E. (2015). Approaches to validation and evaluation in qualitative studies of management accounting. *Qualitative Research in Accounting & Management*, *12*, 230-255. https://doi.org/1109/QRAM-03-2013-0012

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

Kobe, K., & Schwinn, R. (2018). *Small business GDP*, 1998-2014. Washington DC: U.S. Small Business Administration. https://cdn.advocacy.sba.gov/wpcontent/uploads/2018/12/21102039/rs444-Small-Business-GDP-1998-20141.pdf

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2018). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, *100*, 779–796. https://doi.org/10.1016/j.future.2019.05.041

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

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Kremling, J., & Parker, A. M. S. (2017). Cyberspace, Cybersecurity, and Cybercrime. United States: SAGE Publications.

Kulig, T. C., Cullen, F. T., Wilcox, P., & Chouhy, C. (2019). Personality and adolescent school-based victimization: do the big five matter?. *Journal of school violence*, *18*(2), 176-199.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*, 4-13. https://doi.org/10.1108/09685221011035223

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber-crime on the financial sector. *Information and Computer Security*, *45*(2014), 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Latkin, C. A., Mai, N. V. T., Ha, T. V., Sripaipan, T., Zelaya, C., Le Minh, N., & Go, V. F. (2016). Social desirability response bias and other factors that may influence self-reports of substance use and HIV risk behaviors: A qualitative study of drug users in Vietnam. *AIDS Education and Prevention: Official Publication of the International Society for AIDS Education*, *28*(5), 417-425. https://doi.org/1521/aeap.2016.28.5.417

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

Laureani, A., & Antony, J. (2019). Leadership and Lean Six Sigma: A systematic literature review. *Total Quality Management & Business Excellence*, *30*, 53-81.

https://doi.org/10.1080/14783363.2017.1288565

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

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

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Liang, X., Zhao, X., Wang, M., & Li, Z. (2018). Small and medium-sized enterprises sustainable supply chain financing decision based on triple bottom line theory. *Sustainability*, *10*, 4242. https://doi.org/10.3390/su10114242

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

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods*, *30*(3), 191-207. https://doi.org/10.1177/1525822X17749386

Lozupone, V. (2018). Analyze encryption and public key infrastructure (PKI). *International Journal of Information Management*, *38*, 42-44. https://doi.org/10.1016/j.ijinfomgt.2017.08.004

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education, 8*(3), 14. http://ojs.aishe.org/index.php/aishe-j/article/view/335/55\3

Maluf, D. A., Sudhaakar, R. S., & Choo, K. R. (2018). Trust errosion: Dealing with unknown-unknowns in cloud security. *IEEE Cloud Computing, 5*(4), 24-32. https://doi:10.1109/MCC.2018.043221011

Mansfield-Devine, S. (2015). Under the radar. *Network Security*, *12*, 14–18. https://doi.org/10.1016/S1353-4858(15)30112-4

Mangelsdorf, M. E. (2017). What executives get wrong about cybersecurity. *MIT Sloan Management Review, 58*(2), 22-24.

Markey, J. (2018). Don't let hackers impact your small business in 2018. *Fairfield County Business Journal*, *54*(4), 11. https://issuu.com/thewagmag/docs/fair_012218

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

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Martinson, R. (1974). What works? Questions and answers about prison reform. *The Public Interest*, *35*, 22–54.

Matt, C., Hess, T., & Benlian, A. (2017). "Digital Transformation Strategies". *Business &*

Information Systems Engineering, *57*(5), 339–343.

McDermott, C., Isaacs, J., & Petrovski, A. (2019). Evaluating awareness and perception of botnet activity within consumer Internet of Things (IoT) Networks. *Informatics*, *6*(1), 8. https://doi.org/10.3390/informatics6010008

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, *31*, 30-52.

Messner, S. F., Lu, Z., Zhang, L., & Liu, J. (2007). Risks of criminal victimization in contemporary urban China: An application of lifestyle/routine activities theory. *Justice Quarterly*, *24*, 496-522.

Miethe, T. D., & Meier, R. F. (1990). Opportunity, choice and criminal victimization rates: A theory of a theoretical model. *Journal of Research in Crime & Delinquency*, *27*, 243-266.

Miró-Llinares, F., & Johnson, S. D. (2018). Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace. In G. J. N. Bruinsma & S. D. Johnson (Eds.), *The Oxford Handbook of Environmental Criminology* (pp. 883–906). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190279707.013.39

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

Mohammad, T., & Nooraini, I. (2021). Routine activity theory and juvenile delinquency: The roles of peers and family monitoring among Malaysian adolescents. *Children and Youth Services Review, 121*.

https://doi.org/10.1016/j.childyouth.2020.105795

Mohr, J. J., & Metcalf, E. C. (2018). The business perspective in ecological restoration: issues and challenges. *Restoration Ecology*, *26*, 381-390. https://doi.org/.1111/rec.12562

Morgan, S. J., Pullon, S. R. H., Macdonald, L. M., McKinlay, E. M., & Gray, B. V. (2017). Case study observational research: A framework for conducting case 109 study research where observation data are the focus. *Qualitative Health Research*, *27*, 1060-1068. https://doi:10.1177/1049732316649160

Morison, T., Gibson, A. F., Wiggington, B., & Crabb, S. (2015). Online research methods in psychology: Methodological opportunities for critical qualitative research. *Qualitative Research in Psychology*, *12*(3), 223–232. https://doi.org/10.1080/14780887.2015.1008899

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212–1222. https://doi.org/10.1177/1049732315588501

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

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

Munteanu, A. (2017). Running the risk IT – More perception and less probabilities in uncertain systems. *Information and Computer Security*, *25*(3), 345-354.

https://doi.org/10.1108/ICS-07-2016- 0055/

Myers, M. D. (1997). Qualitative Research in Information Systems. *MI Quarterly*, *21*(2), 241. https://doi.org/10.2307/249422

Nadal, K. L., Davidoff, K. C., Davis, L. S., Wong, Y., Marshall, D., & McKenzie, V. (2015). A qualitative approach to intersectional microaggressions: Understanding influences of race, ethnicity, gender, sexuality, and religion. *Qualitative Psychology*, *2*, 147-163. https://doi:10.1037/qup0000026

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice*, *17*, 418–432.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2019a). Cyber Crime: An Existential Threat to Small Business, https://www.nist.gov/speech-testimony/cyber-crime-existential-threat-small-business

National Institute of Standards and Technology (2021). Cybersecurity Framework: Uses and Benefits of the Framework, https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework

National Institute of Standards and Technology. (2019b). Small Business Cybersecurity: Federal Resources and Coordination, https://www.nist.gov/speech-testimony/small-business-cybersecurity-federal-resources-and-coordination

Newington, L., & Metcalfe, A. (2014). Factors influencing recruitment to research: Qualitative study of the experiences and perceptions of research teams. *BMC Medical Research Methodology, 14*, 1-20. https://doi.org/1186/1471-2288-14-10

Ngoqo, B., & Flowerday, S. (2015). Information Security Behavior Profiling Framework (ISBPF) for student mobile phone users. *Computer Security, 53*, 132-142.

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

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), 1-13. https://doi.org/1177/1609406917733847

O'Connell, S., McCarthy, V. J. C., & Savage, E. (2018). Frameworks for self-management support for chronic disease: A cross-country comparative document analysis. *BMC Health Services Research*, *18*(583), 1-10. https://doi.org/10.1186/s12913-018- 3387-0

Osborn, E., & Simpson, A. (2017). Risk and the small-scale cyber security decision making dialogue – a UK case study. *The Computer Journal*, *61*(4), 1-24.

Palmas, W. (2018). Who protects participants in non-inferiority trials when the outcome is death. *Research Ethics*, *14*(1), 10-15. https://doi.org/1177/1747016118764304

Patterson, J. (2017). Cyber-Security Policy Decisions in Small Business (Doctoral Dissertation).

Park, K., Woo, S., Moon, D., & Choi, H. (2018). Secure cyber deception architecture and decoy injection to mitigate the inside threat. *Symmetry*, *10*(1), 14. https://doi.org/10.3390/sym10010014

Patton, M. Q. (2015). Qualitative Research & Evaluation Methods, 4th Ed. Thousand Oaks, CA: Sage Publications.

Paulsen, C. (2016). Cybersecuring small business. *Computer*, *49*(8), 92-97. https://doi.org/10.1109/MC.2016.223

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

Philip, J., & Salimath, M. S. (2018). A value proposition for cyberspace management in organizations. *Business Information Review*, *35*(3), 122–127. https://doi.org/10.1177/0266382118791253

Ponemon Institute. (2018). Cost of a data breach study. https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/

Ponelis, S. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Research*, *10*, 535-550. https://doi.org/10.28945/2339

Ponemon Institute. (2019). 2019 Global State of Cybersecurity in Small and Medium-Sized. Businesses. "Password & Secrets Management | Keeper Security." https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf

Posukhova, O., & Zayats, P. (2014). Social engineering as a mechanism of optimization of human resources management in Rostov region. *Middle East Journal of Scientific Research, 19,* 424-428. https://doi.org/10.5829/idosi.mejsr.2014.19.3.13688

Pozzebon, M., & Rodriguez, C. (2014). Dialogical principles for qualitative inquiry: A nonfoundational path. *International Journal of Qualitative Methods*, *2014*(13), 293–317. https://ejournals.library.ualberta.ca/

Prajogo, D., Toy, J., Bhattacharya, A., Oke, A., & Cheng, T. C. E. (2018). The relationships between information management, process management and operational performance: Internal and external contexts. *International Journal of Production Economics, 199*, 95-103. https://doi.org/10.1016/j.ijpe.2018.02.019

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, 11(3), 335–354. https://doi.org/10.1080/15564886.2015.1057351

Prior, M. (2017). Accomplishing "rapport" in qualitative research interviews: Empathic moments in interaction. Special Issue: The social life of methods, Guest Editors: Gabriele Kasper and Steven J. Ross. *Applied Linguistics Review*, *9*(4), pp. 487-511. https://doi.org/10.1515/applirev-2017-0029

Pyrooz, D. C., Descker, S. H., & Moule, J. R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, *32*(3), 471–499. https://doi.org/10.1080/07418825.2013.778326

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs.

automated cybersecurity anti-phishing techniques. *Computer Science Review, 29*, 44-55. https://doi.org/10.1016/j.cosrev.2018.05.003

Qiao, H. (2018). A brief introduction to institutional review boards in the United States. *Pediatric Investigation*, *2*(1), 46-51. https://doi.org/10.1002/ped4.12023

Radchenko, A., Kolodeznaia, G., & Karpovich, I. (2019). Solving the problem of income loss in the networks of the transport telecommunications operator when providing the VPN service. In *International Scientific Siberian Transport Forum* (pp. 233-244). https://doi.org/10.1007/978-3-030-37916-2_24

Radziwill, N., & Benton, M. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. *Software Quality Professional*, *19*(4), 25-36. http://www.asq.org

Raghavan, K., Desai, M., & Rajkumar, P. (2017). Managing cybersecurity and e-commerce risks in small businesses. *Journal of Management Science and Business Intelligence*, *2*(1), 11. https://doi.org/10.5281/zenodo.581691

Raineri, E., & Fudge, T. (2019). Exploring the sufficiency of undergraduate students' cybersecurity knowledge within top universities' entrepreneurship programs. *Journal of Higher Education Theory and Practice*, *19*(4), 73-92. https://doi-org.ezp.waldenulibrary.org/10.33423/jhetp.vl9i4.2203

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

https://doi.org/10.1016/j.ijans.2018.05.002

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research, 28*, 824-831. https://doi.org/1177/1049732317753586

Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119-1139. https://doi.org/10.1177/0306624x15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber-lifestyle—Routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*, 1149-1169.

Ricci, J., Breitinger, F., & Ibrahim, B. (2019, January). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*(1). https://doi.org/10.1007/s10639-018-9765-8

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation, and prevention. *International Management Review*, *13*(1), 10-21. http://www.scholarspress.us/

Robinson, O. D. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*(1), 25–41. https://doi.org/1080/14780887.2013.801543

Ross, M. W., Iguchi, M. Y., & Panicker, S. (2018). Ethical aspects of data sharing and research participant protections. *American Psychologist*, *73*(2), 138. https://doi.org/1037/amp0000240

Rothrock, R. A., Kaplan, J., & van der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12-15.

Rowley, L. (2019). The value of threat intelligence. *Computer Fraud &Security*, 2019(10), 20. https://doi.org/10.1016/S1361-3723(19)30109-5

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

Ryan, J. C. H. J., Mazzuchi, A. T., Ryan, J. D., Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, *39*, 774–784. https://doi.org/10.1016/j.cor.2010.11.013.132

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers and Data*, 65-78. http://eprints.um.edu.my/13726/1/1-s2.0-S0167404815000863-main.pdf

Saber, A. (2016). Determining small business cybersecurity strategies to prevent data breaches (Doctroal Dissertation).

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

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, *52*(4), 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Savin-Baden, M., & Major, C. (2013). Qualitative research: The essential guide to theory and practice. New York, NY: Routledge.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

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

Schoemaker, P. J., Heaton, S., & Teece, D. (2018). Innovation, dynamic capabilities, and leadership. *California Management Review*, *61*(1), 15-42. https://doi.org/10.1177/0008125618790246

Sechel, S. (2017). Web applications vulnerability management using a quantitative stochastic risk modeling method. *Informatica Economica*, *21*(3), 16-30. https://doi.org/10.12948/issn14531305/21.3.2017.02

Selznick, L. F., & LaMacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology*, *13*(2), 281- 219. https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1289&context=jtl

Sen, R., & Borle, S. (2015). Estimating the context risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341.

https://doi.org/10.1080/07421222.2015.1063315

Sepulveda, D. A., & Khan, O. Q. (2017). A system dynamics case study of resilient response to IP theft from a cyber-attack. 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 1291--1295.

Shapiro, S. J., & Oystrick, V. (2018). Three steps towards sustainability: Spreadsheets as a data collection analysis system for non-profit organizations. *Canadian Journal of Program Evaluation*, *33*(2), 247-257. https://doi.org/10.3138/cjpe.31157

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

Small Business Administration. (2018). Small Business Cybersecurity, https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity

Small Business Association. (2021). Small Business Cybersecurity, https://www.sba.gov/topbusiness-trends-2021

Snape, D., Kirkham, J., Britten, N., Froggatt, K., Gradinger, F., Lobban, F., Popay, J., Wyatt, K., & Jacoby, A. (2014). Exploring perceived barriers, drivers, impacts, and the need for evaluation of public involvement in health and social care research: A modified Delphi study. *BMJ Open, 4*(6), 1–11. https://doi.org/10.1136/bmjopen-2014-004943

Snape, D., Kirkham, J., Britten, N., Froggatt, K., Gradinger, F., Lobban, F., Popay, J., Wyatt, K., & Jacoby, A. (2019). Office of Advocacy: Frequently Asked

Questions. Washington DC: U.S. Small Business Administration. https://www.sba.gov/advocacy

Spicker, P. (2018). The Real Dependent Variable Problem: The Limitations of Quantitative Analysis in Comparative Policy Studies. *Social Policy & Administration*, *52*, 216-228. https://doi.org/1111/spol.12308

Sravanthi, R., & Nisha, T. N. (2021). Moving from Detection Centric to Prevention Centric Security Using Automation: A Survey. *Journal of Physics: Conference Series*, *1964*(4)https://doi.org/10.1088/1742-6596/1964/4/042048

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

Stewart, A. (2018). A utilitarian re-examination of enterprise-scale information security management. *Information and Computer Security*, *26*(1), 39-57. https://doi.org/10.1108/ICS-03- 2017-0012

Sturmberg, J. P., Martin, C. M., & Katerndahl, D. A. (2014). Systems and complexity thinking in the general practice literature: An integrative, historical narrative review. *Annals of Family Medicine*, *12*, 66-74. https://doi.org/10.1370/afm.1593

Sun, J., Wu, S., & Yang, K. (2018). An ecosystemic framework for business sustainability. *Business Horizons*, *61*, 59-72. https://doi.org/10.1016/j.bushor.2017.09.006

Sutton, M. (2018). Routine activity theory: "Mindless" chemistry meme masquerades as a theory of crime causation. *Internet Journal of Criminology*.

https://dysology.org/page8.html

The White House. (2009). National Cybersecurity Awareness Month, 2009 https://www.whitehouse.gov/the_press_office/PresidentialProclamation

Thomann, E., & Maggetti, M. (2017). Designing research with qualitative comparative analysis (QCA): Approaches, challenges, and tools. *Sociological Methods, & Research*, 004912411772970. https://doi.org/10.1177/0049124117729700

Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*, 23-41. https://doi.org/10.1080/14780887.2016.1219435

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

Thomas, J., & Galligher, G. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. *Computer and Information Science*, (11). https://ssrn.com/abstract=3095629

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

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

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

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

Tyler, L. B. (2018). Exploring the implementation of cloud security to minimize electronic health records cyberattacks (Doctoral Dissertation).

US-CERT. (2020, August 25). Avoiding social engineering and phishing attacks. https://www.us-cert.gov/ncas/tips/ST19-001

U.S. Department of Commerce. (2017). Small Business Cybersecurity: Federal Resources and Coordination. Gaithersburg, MD. https://www.nist.gov/speech-testimony/small-business-cybersecurity-federalresources-and-coordination

U.S. Department of Energy. (2018). DOE Cybersecurity Strategy and Implementation Plan. https://www.doe.gov/sites/default/files/publications/implementation plan/HandbookAttachment.pdf

U.S. Department of Homeland Security. (2012). DHS 4300A sensitive systems handbook. https://www.dhs.gov/sites/default/files/publications/4300A-HandbookAttachment-S1-Managing-CREs-Containing-SPII.pdf

U.S. Department of Homeland Security. (2015). DHS 4300A sensitive systems handbook. https://www.dhs.gov/sites/default/files/publications/4300A-HandbookAttachment-S1-Managing-CREs-Containing-SPII.pdf

Usman, M., Jan, M. A., He, X., & Chen, J. (2019). A survey on representation learning efforts in cybersecurity domain. *ACM Computing Surveys* (CSUR), *52*, 111-112. https://doi.org/10.1145/3331174

Vakhitova, Z. I., Alston-Knox, C., Danielle, R., Townsley, M., Webster, J. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior, 101, 225-237.* https://doi.org/10.1016/j.chb.2019.07.012

Von Bertalanffy, L. (1969). General system theory: Foundations, development, applications. New York, NY: George Braziller.

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

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

Walters, I. (2017). Strategies for recruiting cybersecurity professionals in the financial service industry (Doctoral Dissertation).

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

Watson, T. (2018). Ethnography and the management of organizations. In: Ciesielska M., Jemielniak D. (eds) Qualitative Methodologies in Organization Studies. Palgrave Macmillan, C. https://doi.org/10.1007/978-3-319-65217-7_6

Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based leadership development: Insights from expert coaches. *Consulting Psychology Journal: Practice & Research*, *66*(1), 20–37. https://doi.org/1037/cpb0000002

Wen-qun, X. (2006). The design of cybercrime spatial management system based on GIS. *Geographical Research*, *25*(5), 948–952.

Wertheim, S. (2019). Auditing for cybersecurity risk: Certified public accountant. *The CPA Journal*, *89*(6), 68-71. https://ezp.waldenulibrary.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fauditing-cybersecurity-risk%2Fdocview%2F2239577276%2Fse-2%3Faccountid%3D14872

West, J. (2017). Fundamentals of a cybersecurity program. Internal auditors and information security professionals can join forces to prepare the organization for cyber threats. *Internal Auditor*, *74*(6), 16-17.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Wilkerson, J. M., Iantaffi, A., Grey, J. A., Bockting, W. O., & Rosser, B. R. S. (2014). Recommendations for internet-based qualitative health research with hard to Reach populations. *Qualitative Health Research*, *24*(4), 561–574. https://doi.org/10.1177/1049732314524635

Wirth, A. (2017). The economics of cybersecurity. *Biomedical Instrumentation & Technology*, 52-59.

Wolverton, C., & Stevens, D. (2019). The impact of personality in recognizing disinformation. *Online Information Review*, *44*(1), 181-191. https://doi.org.ezp.waldenulibrary.org/10.1108/OIR-04-2019-0115

Xiong, X. -L., Yang, L., & Zhao, G. -S. (2019). effectiveness evaluation model of moving target defense based on system attack surface. *IEEE Access*, *7*, 9998–10014. https://doi.org/10.1109/ACCESS.2019.2891613

Yadav, A., Yadav, R., & Tiwari, M. (2020). Website security for detection and prevention of attacks. *I-Manager's Journal on Software Engineering*, *14*(3), 37-41. https://doi.org.ezp.waldenulibrary.org/10.26634/jse.14.3.17360

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

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

Yin, R. K. (1981). The Case Study as a Serious Research Strategy. Knowledge: Creation, Diffusion, Utilization. *Sage Publication Science Communication*, *3*(1), 97-114 https://journals.sagepub.com/doi/10.1177/107554708100300106

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage Publications.

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

Yip, C., Han, N. R., & Sng, B. L. (2016). Legal and ethical issues in research. *Indian Journal of Anaesthesia*, *60*(9), 684-688. https://doi.org/10.4103/0019-5049.190627

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *2018*(108), 107-118. https://doi:10.1016/j.dss.2018.02.009

Young, A., & Yung, M. (2017). Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM*, *60*(7), 24-26. https://doi.org/10.1145/3097347

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

Appendix A: Open-Ended Interview Questions

The method of data collection from the study includes ten open-ended questions in a virtual face-to-face interview with a possibility of six additional questions related to scarcely utilized strategies of small business cybersecurity analysts to gather the data:

1. What methods do you use to protect your systems from external cybersecurity threats?
2. What are the challenges in obtaining C-level support for providing effective cybersecurity strategies in your organization?
3. What inefficiencies or lack of resources do you and your team experience utilizing industry-standard cybersecurity measures to prevent cybersecurity threats in your organization?
4. What industry-standard cybersecurity strategies effectively prevent inefficiencies as you protect the organization from cybersecurity threats?
5. What challenges do you and your team experience in utilizing industry-standard cybersecurity strategies in the prevention of cybersecurity threats?
6. What cybersecurity strategies do you and your team apply in the prevention of cybersecurity threats?
7. Which cybersecurity strategies are the most effective in reducing inefficiencies in the prevention of cybersecurity threats?
8. What other challenges or inefficiencies do you experience in adopting an industry-standard model to prevent cybersecurity threats?

9. What are the factors when selecting industry-standard cybersecurity strategies to prevent cybersecurity threats?
10. What additional information can you provide about strategies to prevent breaches and cybercrime within your organization?

Please note: The researcher plans to take notes of observations during the interview.

Six additional questions may be added here as informed by the answers from the interview.

1. Why are cyber-attacks more prevalent in your organization?
2. What are some deterrents to prevent hackers from targeting your organization?
3. How does your organization apply defense in depth?
4. What is the most prevalent attack in your organization?
5. Has your organization considered varying the routine activities of people, processes, and technology as a deterrent? Why? Why not?
6. What are some ways to deter the motivations of the attacker?

Appendix B: Interview Protocol

The semistructured face-to-face virtual interview includes the following process:

1. Introduction of the research topic as stated in the "Informed Consent" form and provide a copy of the form;
2. Presentation of the recording device to the participant;
3. Assure the participant of confidentiality;
4. Confirm the interview process will take no longer than 60 minutes;
5. Encourage the participant to answer the questions to their best ability
6. Restate the questions and answers of each participant when applicable.
7. Note any expanding questions for future interviews to maintain reliability and validity in the collection of data;
8. Note any observations during the interview;
9. Thank each participant at the end of the interview;
10. I will inform the participant that I will transcribe the interview from the audio recording and email them a one to two-page summary of the interview in a process called member checking, where they approve the data collected for analysis;
11. I will schedule a follow-up interview via telephone call if necessary to verify the data collected is accurate unless I receive an email from you that the verifying the summary is correct; and
12. Review and analyze relevant industry standard documentation.

Appendix C: Online Ordinal Process for Face-to-Face Interview

1. Introduce the research topic;
2. Explain the consent form (see Appendix A);
3. Present the recording device;
4. Emphasize confidentiality;
5. Gain verbal approval from the participants to record the interview;
6. Confirm the interview will take no longer than 60 minutes;
7. Encourage participants to answer questions to the best of their ability; and
8. Thank each participant upon completion of the interview for the contribution to the study.