2022

Strategies for Cybercrime Prevention in Information Technology Businesses

Sophfronia G. Tucker
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Sophfronia G. Tucker

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. Erica Gamble, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Jonathan Schultz, Committee Member, Doctor of Business Administration Faculty

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

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

Walden University
2022

Abstract

Strategies for Cybercrime Prevention in Information Technology Businesses

by

Sophfronia G. Tucker

MBA, Kaplan University, 2008

MS, North Carolina State University, 1987

BS, Benedict College, 1983

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

July 2022

Abstract

Cybercrime continues to be a devastating phenomenon, impacting individuals and businesses across the globe. Information technology (IT) businesses need solutions to defend and secure their data and networks from cyberattacks. Grounded in general systems theory and transformational leadership theory, the purpose of this qualitative multiple case study was to explore strategies IT business leaders use to protect their systems from a cyberattack. The participants included six IT business leaders with experience in cybersecurity or system security in the Midlands region of South Carolina. Data were collected using semistructured interviews and reviews of government standards documents; data were analyzed using thematic analysis. Three themes emerged from the study: (a) cybercrime prevention strategy; (b) cybersecurity awareness, training, and education; and (c) effective leadership. A key recommendation is for IT business leaders to ensure employees are current on cybersecurity awareness and defense techniques through regular training and education, use third-party vendors that are subject matter experts where they lack talent, and develop leaders with a transformational mindset. The implications for positive social change include the potential for IT business leaders and employees to become more proactive in learning and implementing effective cybercrime prevention strategies to keep their businesses profitable and support the needs of stakeholders and clients.

Strategies for Cybercrime Prevention in Information Technology Businesses

by

Sophfronia G. Tucker

MBA, Kaplan University, 2008

MS, North Carolina State University, 1987

BS, Benedict College, 1983

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

July 2022

Dedication

This doctoral work is dedicated to my late mother, Mrs. Emmie Richardson Tucker, who passed away before I was able to embark on this journey, but she always knew it was a desire in my heart. And to my Aunt Rene Richardson Kettrell who helped fill the gap and kept asking me, “Now when are you going to be a doctor?” Thank you.

Acknowledgments

I first acknowledge Jesus Christ as my Lord and Savior for his many blessings and all that He has done to enable me to achieve this goal. A special thank you to my husband, Charles B. Harrell, who had to endure a lot as I spent countless hours on my computer and had no time for him. Nonetheless, he kept encouraging me to finish and loved me unconditionally. To one of my besties Paula Perry: who prayed, encouraged, and even let me use her printer at work to print my study. To my longtime friend Charles Peterson, who believed in me from day one and continued to encourage me to finish every opportunity he had.

I have much gratitude and appreciation for my committee chair Dr. Erica Gamble for her pushing, correction, encouragement, and words of wisdom. Thank you from the bottom of my heart. I would also like to thank the many others in the Walden family who gave corrections, words of support, and encouragement. I could not have made it without you: Dr. Schultz, the Walden University editors, university research reviewer committee, and my Walden University cohort classmates.

Finally, I give thanks to my participants, friends, family, and the Women of Purpose prayer team whose prayers availed much on this journey. Each of you played a significant part in helping me obtain this degree, and I will always be grateful. I will forever be grateful for the deposits you have made into my life. May God bless each of you.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Data breaches have become a frequent occurrence, affecting businesses on a large-scale globally (Cross et al., 2019). Business leaders have realized how destructive a cyberattack can be on an organization (Wilding, 2016). The impact of cyberattacks on businesses have brought many daily operations to a standstill, compounded by a damaged reputation (Govender et al., 2021). To mitigate the harmful effects of cybercrime activity against a business, information technology (IT) managers should understand the best strategies needed to help protect company networks in a cyberattack.

Background of the Problem

The internet, also known as cyberspace, is growing at a phenomenal rate, and so are cybercrimes (Nasution et al., 2018). With the evolution of the internet and personal computers, businesses have become more productive in faster transactions, exposure to e-commerce, better communication, and improved marketing techniques (Rana, 2018). Although advancements in technology improve the conduct of business, these advancements also can increase security breaches known as *cybercrimes* (Arcuri et al., 2017). Cyberattacks in the 21st century are not about simple annoyance or defacing a website, but attackers are aiming to steal and destroy confidential company data by targeting specific organizations (Kessler & Ramsay, 2013). Government agencies and businesses are becoming victims of cybercrime daily (Iovan & Iovan, 2016). Because of the increase in cybercrime activities, in 2009, President Obama declared networks and computers as national assets to have prioritized protection (Robinson et al., 2015).

Problem Statement

Data breaches have become a frequent occurrence, affecting businesses on a large-scale globally (Cross et al., 2019). According to Kurpjuhn (2019), the number of cyberattacks targeted explicitly at businesses continues to rise. Business leaders realize how much damage a cyberattack can have on an organization (Wilding, 2016). To mitigate harmful effects of cybercrime activity against a business, IT managers should understand the best strategies necessary to protect companies in the event of a cyberattack.

Purpose Statement

The purpose of this qualitative multiple case study was to explore effective cybercrime prevention strategies that IT business leaders use to protect their businesses from cyberattacks. The targeted population was IT business leaders in companies located in the Midlands region of South Carolina, who have implemented effective strategies that protect their businesses from cyberattacks. This research has potential implications for positive social change that include creating an environment wherein consumers are more confident to conduct business with IT companies, which may stimulate the economy positively, resulting in improved financial resources for providing social infrastructures such as schools and hospitals for the community.

Nature of the Study

In this study, I elected to use a qualitative methodology approach to research strategies that business leaders use to protect their networks from cyberattacks. With the qualitative research approach, a researcher gains in-depth knowledge of human

behaviors, attitudes, and motivations to make sense of their experiences and the environment in which they live (Holloway & Galvin, 2017). Quantitative researchers primarily test hypotheses and use statistical facts to measure and explain a social phenomenon (Baskarada, 2014; Yin, 2018). Mixed-methods researchers employ both qualitative and quantitative research methods to achieve research objectives (Krawczyk et al., 2017). To explore effective cybercrime prevention strategies for businesses, I did not test a hypothesis, nor did I use a combination of both quantitative and qualitative methods.

I evaluated three research designs optional for conducting qualitative research on cybercrime prevention strategies: ethnography, phenomenology, and case study. Ethnography requires researchers to become engaged in the lives of the participants for an extended period, learning about their culture in a specific context (Marion et al., 2015). I did not choose ethnography because my goal was not to understand the cultural norms of a group of people. With phenomenology, the objective of researchers is to understand and capture the lived experiences of participants (Kruth, 2015). The phenomenological design was not relevant to this study because I did not need to explore the lived experiences of the participants. A case study design allows a researcher to perform rigorous research, gaining an in-depth understanding of the field of interest (Houghton et al., 2015). A multiple case study is most suitable for answering *how* and *what* questions about a phenomenon within a real-life context (Baskarada, 2014; Yin, 2018). Additionally, a multiple case study serves in replication of findings (Ridder,

2017); therefore, I chose the multiple case study design to understand the phenomenon of cybercrime prevention in a real-life context.

Research Question

What effective cybercrime prevention strategies do IT business leaders use to protect their businesses from cyberattacks?

Interview Questions

1. What cybercrime prevention strategies do you use to protect your business from a cyberattack?
2. What type of cybercrime prevention education and training do you provide for your employees on a routine basis?
3. What is your contingency plan if a cyberattack occurs?
4. What strategies are most effective in training employees to implement safe cybersecurity practices?
5. What strategies do you use to enforce the use of safe cybersecurity practices by your employees when they work from home or off-site?
6. What procedures do you use to ensure that your cybersecurity policies are current?
7. What strategies have you implemented that are most effective in preventing insider data leakage?
8. What specific leadership strategies do you use to implement your current cybercrime prevention strategies?

9. What transformational skills do you use to encourage your employees to adhere to safe cybersecurity practices?
10. What other information would you like to share regarding cybercrime prevention strategies that IT business leaders use to protect their businesses from cyberattacks?

Conceptual Framework

I used general systems theory (GST) by von Bertalanffy (1968) and Burns' (1978) theory of transformational leadership as the conceptual framework for this study, to assist with theme identification and interpretation of data analysis. In 1972, GST became popular as a method for analyzing and understanding complex systems (Montgomery & Oladapo, 2014). GST functions as the foundation for viewing phenomena, patterns, and proclivities in real-life scenarios (Whitney et al., 2015). Von Bertalanffy believed that GST could be used as a broad scope of inquiry for all relevant factors to achieve a specific end. Young and Levenson (2014) suggested using systems theory as the framework for implementing cybersecurity systems and loss prevention strategies. In this study the GST framework was used as a basis to explore complex IT systems and the implementation of cybercrime prevention strategies used by IT business leaders.

Burns (1978) initially established the theory of transformational leadership, with emphasis on meeting basic needs and desires that inspire followers to create new solutions and enhance their workplace. Critical constructs of the transformational leadership theory are idealized influence, intellectual stimulation, individualized consideration, and inspirational motivation (Ghasabeh et al., 2015). Bhattacharya (2011)

revealed that transformational leaders are most effective in developing information security policies, system activity monitors and developing antivirus software. By applying the theory of transformational leadership to this study, I explored how transformational characteristics of business leaders may influence the implementation of cybercrime prevention strategies.

Operational Definitions

Data breach: An incident in which hackers or unauthorized users steal data or private information in a cyberattack for malicious intent (Cheng & Walton, 2019).

Denial-of-service (DoS): A malicious attack that denies legitimate users the access of network connections of a company by overloading resources or the machine, through transmitting many packets that cause the system to crash or perform very slowly (Amiri & Soltanian, 2015).

Distributed denial-of-service (DDoS): A more complex version of DoS known for using multiple attack methods, with the capability to overwhelm a web server, slowing down the speed and potentially halting the entire system (Jaafar et al., 2019).

Game theory: The study of how multiple agents or players interact among themselves to obtain the best outcome in a situation (Argan et al., 2022).

Insider threat: A description of a trusted partner or an employee of an organization who maliciously and intentionally causes harm to the organization's network, resources, and data (Chattopadhyay et al., 2018).

Phishing: The deceptive or fraudulent practice of sending emails by an attacker to trick a victim into releasing sensitive information such as username, password, personal identification number (PIN), or other personal data for unauthorized use (Kolouch, 2018).

Assumptions, Limitations, and Delimitations

Assumptions are preliminary beliefs accepted as true without having proof (Yang et al., 2018). According to Merriam (2014), assumptions are facts believed to be correct but not verified by the researcher. Identified assumptions are not a warrant to accept anything but they provide support of a researcher's methodological decisions (Wolgemuth et al., 2017). To explore cybercrime prevention strategies used by IT business leaders, I made three assumptions. The first assumption was that participants had a sincere interest in participating in the interview process to help reduce or deter future cybercrime attacks. Another assumption was that each participant would provide truthful and accurate information on the cybersecurity practices used in their business. The third assumption was that the answers provided in the interviews would enable me to gain truthful insights into cybercrime prevention strategies.

Limitations are factors that set the boundaries of a study and how the results of the study may or may not contribute to understanding the research (Busse et al., 2016). A potential limitation was that selected participants would have limited experience in handling cyberattacks and developing cybercrime prevention strategies. In addition, the number of participants interviewed was limited to the available IT businesses located in the Midlands region of the state of South Carolina. Participants may have been held to a certain level of confidentiality within their businesses because of any ongoing

cyberattack investigations. Finally, the COVID-19 pandemic may have placed a limit on the number of participants who were comfortable participating in interviews.

Delimitations define the parameters of a study, a researcher's decisions, and the rationale behind such decisions (Marshall & Rossman, 2016). Delimiting factors may be comprised of variables of interest, sample size, research questions, and the adopted theoretical framework (Wolgemuth et al., 2017). The first delimiter in this study included IT business leaders who have implemented cybersecurity strategies within the last 5 years. The second delimiter included choosing a subset of IT business professionals with a minimum of 2 years of leadership experience in cybersecurity or network security. Finally, I limited the selection of purposive sampling to the Midlands region of the state of South Carolina, based upon referrals and accessibility.

Significance of the Study

Businesses that are victims of a cyberattack may find themselves facing the risk of theft, fines, reputational damage, and financial losses that affect their profits (Arcuri et al., 2017). Findings from this study may provide community leaders, stakeholders, and academic personnel with pertinent data to develop relevant cybersecurity strategies. The results from this study may also benefit IT businesses, stakeholders, and customers. IT business leaders may become equipped with a viable cybercrime prevention plan of resilience to combat potential cyberattacks.

Contribution to Business Practice

Tounsi and Rais (2018) noted that a new line of cybersecurity is necessary as cyberattacks become more aggressive. IT business leaders could benefit from this study

by understanding effective cybercrime prevention strategies that protect company assets in the event of a cyberattack. Factual evidence discovered by business practitioners might be relevant for protecting a firm's value following data breaches (Gwebu et al., 2018). Improving the cybercrime prevention strategies implemented by IT business leaders to protect against cyberattacks could be an additional contribution to business practices. The results of this study might engender improvement of the education curriculum and become a contribution to the existing pool of knowledge on cybersecurity.

Implications for Social Change

The rise in cybercrime is evidence of the increased number of targets on the internet, the high risk, and the need for protection of those attacked (Conteh & Royer, 2016). The implications for social change of this study include the possibility of IT business leaders experiencing greater awareness and education on cybercrime prevention strategies to protect their systems in the event of a cyberattack or data breach. Businesses may safely expand in the community, resulting in increased jobs and improvement of the local economy or society.

A Review of the Professional and Academic Literature

A literature review is a comprehensive understanding and critical analysis of previous research that provides knowledge about a topic of study or research question (Machi & McEvoy, 2016). The objective of this qualitative multiple case study was to explore effective strategies for cybercrime prevention among IT businesses. I researched literature and performed a detailed analysis of various forms of data to become informed on the subject matter. I organized the literature review into the following headings: (a)

expansion of the conceptual framework, (b) the financial and economic impact of cybercrime, (c) cyber insurance and cyber talent, (d) types of cybercrime attacks, (e) other methods of cyberattacks, (f) cybercrime prevention strategies, (g) cyber resilience, (h) response strategies, (i) insider threats, (j) education and training, and (k) legal aspects of cybercrime.

The strategy for researching the literature was the use of search criterion that included the following keywords or phrases: *data breach, security fraud, cybercrime, data theft, computer crimes, data loss, cyberattack, data security, cybersecurity, network security, general systems theory, game theory, transformation leadership theory, IT/information technology, IS/information security and systems,* and *IT businesses*. My review consisted of in-depth research of scholarly resources that included peer-reviewed journal articles, dissertations, electronic media, and books from various databases, libraries, and search engines. I retrieved information from Google Scholar, Richland County Public Library, and Walden University Library with links to ProQuest, IEEE Source Library, Business Source Complete, Emerald Insight, SAGE Premier, and EBSCOhost. I also retrieved information from the following government sites: U.S. Department of Homeland Security, the White House, National Security Agency, National Institute of Standards and Technology (NIST), U.S. Department of Defense, and Federal Bureau of Investigation (FBI).

This search resulted in more than 200 resources. After applying additional filters for current dates (published within 5 or 6 years) and evaluation for relevancy to the study, I retained 201 articles. The references for this study include 169 peer-reviewed journal

articles, seven articles from sources that are not peer reviewed, five conference reports, nine books, four websites and four dissertations related to my doctoral study. These resources were relevant to answering the general research question.

Conceptual Framework

I used GST and the transformational leadership theory as viewing lenses for researching the central business problem. I critically reviewed supporting and opposing theories regarding the topic of cybercrime prevention, including servant leadership and game theory. The premise of the servant leader is to serve others first, which in turn results in the growth of being served (Keets & Abaldo, 2017). According to Martin et al. (2017), the servant leader is an effective listener with the ability to accept the views of others and their needs and motivations, which gives them the ability to understand better and target the needs of their followers. The approach in game theory is to view cybercrime prevention primarily from a defense mechanism perspective. Note, game theory provides the answer to how defenders respond to an attack in cybersecurity (Do et al., 2017).

General Systems Theory

Von Bertalanffy formulated the notion of GST as early as the 1930s. Von Bertalanffy postulated GST as a mathematical field that provides for the formation and derivation of principles applied to systems in general. GST was conceptualized as a theory and conceptual framework that could be applied to many fields of study (Idahosa, 2020). Von Bertalanffy believed that every organization is a system made up of a complex set of elements interacting together (Edmonds, 2017; Hammond, 2010;

Lopreato, 1970). Broad classifications are *open* and *closed* systems (von Bertalanffy, 1968). Business organizations are classified as open systems because of their characteristics of synergy, entropy, and subsystem interdependence (Iwu et al., 2016).

Cybercrime continues to affect a broad section of the world. To help manage cybersecurity risks more effectively, researchers have identified the need to view cybersecurity holistically from the lens of system thinking: the discipline for seeing wholes (Tarafdar & Bose, 2019). Von Bertalanffy (1968) explained the holistic approach in GST as a system comprised of interrelating parts, where all parts are never viewed as a single part. In GST, the exploration of wholes and wholeness (von Bertalanffy, 1972) and organizational evaluation stem from the framework of observing interrelationships rather than objects and for seeing changing versus static patterns (Tarafdar & Bose, 2019). Business organizations are comprised of many independent units that work together as a whole to accomplish organizational goals. Therefore, GST was used to show how IT business leaders and their subordinates work together to develop cybercrime prevention strategies.

GST provided a framework for evaluating the interaction between parts of a system, such as the internet and organizations. When evaluating an organization, several elements of systems theory may be applicable (Mania-Singer, 2017). GST emphasizes that the structure of organizations is composed of a series of related subsystems (Mania-Singer, 2017). GST classifies organizations as open systems, which are characterized by an inflow and outflow that changes the components of the system (Mania-Singer, 2017; von Bertalanffy, 2008). The continuous exchange of energy and matter causes significant

differences with the environment, which would enable IT business leaders to provide better protection of critical infrastructure.

Rousseau (2015) noted that the founders of GST believed in the theory's ability to contribute to a scope of science that could be used to build a better world through systematic innovation. Von Bertalanffy described systems theory as a mathematical discipline connected to computers and modern technical systems (Hammond, 2010). The application of GST may identify and reveal computational and information-processing systems as described by Katrakazas et al. (2020). Lyon (2020) suggested GST as a supportive theory used by all cultures, including corporate cultures, to analyze and understand core values and assumptions. Viewing cybercrime through the lens of GST, IT business leaders may discover new insights and strategies for cybercrime prevention.

Transformational Leadership

Burns (1978) introduced the concept of transformational leadership as a process in which the motivation and moral values of leaders and followers are heightened to higher standards (Yasir & Mohamad, 2016). In 1985, Bass expanded the work of Burns to further define the theory of transformational leadership based on the four dimensions of (a) idealized influence, sharing of vision and overall mission; (b) inspirational motivation, building employee confidence and enthusiasm toward higher goal achievement; (c) individualized consideration, employee recognition of needs; and (d) intellectual stimulation, challenges that require employees to think at a higher level (Bass, 1985; Brown et al., 2019; Crane & Hartwell, 2018). Transformational leaders promote

organizational growth by focusing on social responsibility, diversity, and inclusivity (Brown et al., 2019).

Transformational leadership positively influences organizational innovation and empowerment via successful motivational concepts (Chang et al., 2017). Motivation is a core element of transformational leadership, which inspires followers to commit to a common goal (Bronkhorst et al., 2015). Transformational leaders inspire employees by emphasizing the significance of their work and highlighting important corporate goals (Oh et al., 2019). According to Bronkhorst et al. (2015), motivation is the primary factor of job performance and an important element to understand organizational behavior. Khan et al. (2020) noted that transformational leaders directly influence their followers by equipping them with the necessary tools to perform their jobs efficiently. A transformational leader stimulates followers through psychological empowerment and establishing social identification within the organization (Han et al., 2020). A transformation leader influences the development of employees and drives the direction of the organization (Abdul et al., 2019; Crane & Hartwell, 2018). In transformational leadership, the transformation approach redesigns perceptions, values, and aspirations, creating significant change that transforms individuals and organizations (Hostrup & Anderson, 2020; Money, 2017).

Managers exhibit different leadership styles that encourage their workers to produce outcomes that are most beneficial to the entire organization (Erkutlu, 2008). A transformational leader gains effective levels of follower commitment and participation by acting as a role model (Yildiz & Simsek, 2016). A transformational leader can inspire

followers by encouraging employees to achieve performance objectives by motivating them to change their mindset and belief systems (Deschamp, 2016). Unlike transactional leadership based on the premise of exchange-based relationships, transformational leaders transform individuals by changing their attitudes, beliefs, and values (Bass, 1985; Purwanto et al., 2020).

Effective leadership serves as the underpinning for healthy and innovative companies, which is a must for creating robust cyber-security strategies (Banks, 2016). Kuusisto and Kuusisto (2016) advised adherence to leadership principles when implementing cybersecurity strategies. Security strategies must be in alignment with the business strategies when implementing leadership decision-making processes in an organization (James, 2018). Cybersecurity is a business strategy for all businesses, requiring senior IT and cybersecurity leaders to become more engaged at the executive level (Toth, 2017). Transformational leadership and GST support the research in exploring effective strategies that IT business leaders use to prevent cybercrime attacks.

Supporting and Contrasting Theories

Servant leadership. Greenleaf (1977) developed the original principles of servant leadership based on the desire to serve. Hoch et al. (2018) stated that Greenleaf believed that a servant leader first serves those they lead. Seto and Sarros (2016) posited that the servant leader promotes, embraces, and demonstrates behaviors that positively influence their followers for the betterment of the organization. Hoch et al. (2018) suggested that servant leaders who first focus on the development and well-being of their followers will gain followers focused on obtaining long-term goals.

A review of the theory of servant leadership revealed similarities to the idea of transformational leadership, along with some distinct differences. According to Stone et al. (2004), both servant and transformational leadership styles share attributes of influence, vision, and trust. One difference in the two leadership styles is the focus of the leader; whereas the servant leader focuses on service to the followers, the transformational leader concentrates on motivating followers to support the objectives of the organization and inspiring follower commitments (Hoch et al., 2018; Stone et al., 2004; Tian et al., 2020). Although servant leadership is a relevant viewing lens for the study of cybercrime prevention strategies, transformational leadership was better suited for this study because of the transforming power to ensure acceptance, buy-in, and compliance with crafted strategies in IT businesses.

Game theory. Cybercriminals see computer systems as tempting targets to attack (Chung et al., 2016). The game theory became a popular viewing lens on how defenders respond to an attack (Do et al., 2017), which differs from GST's holistic approach. The objective of game theory is to look at possible risks of attack in cyberspace, then decide on ways to counterattack or minimize the impact. John Nash, a pioneer of game theory, built this theory on the premise of understanding the moves of the players and a system in a state of equilibrium (Nash, 1997, as cited in Goyal et al., 2018). According to Goyal et al. (2018), a system in equilibrium has all parties making decisions that are in the best interest of everyone involved. Unfortunately, seeking the best interest of others is not the position of cybercriminals, and therefore game theory would not have been the best framework for this study.

Financial and Economic Influence of Cybercrime

Cyberattacks, data breaches, and privacy violations are daily occurrences in businesses (Romanosky, 2016). Globally, the cost of cybercrime is estimated at more than $113 billion yearly (Feuilherade, 2021). Businesses lose money in a plethora of ways from cyberattacks, but one of the most devastating cyber incidents is data breaches. According to Erickson and Neilson (2018), one commercial builder potentially lost more than $1 million when an attacker encrypted files to their servers, making it impossible to access data files needed to compete for a bid. Cybercriminals have impacted IT organizations financially by threatening to disrupt their daily operations and then demand that the organization pay for protection from the attack (Carter, 2016). For instance, a California hospital paid more than $17,000 in bitcoin after the hijack of their system, preventing employees from communicating electronically for 10 days (Carter, 2016).

Gañán et al., (2017) emphasized the importance of understanding the economic impact of cybercrime. Radanliev et al. (2018) posited that the economic implications of cyber-security and its associated risks are of growing importance as IT devices increase in connectivity. No exact figure of financial losses incidental to cybercrime can be identified, although $1 trillion is estimated as an annual figure in financial losses, incurred because of cyber-criminal activity (Radanliev et al., 2018). Statistical research predict businesses will experience more than $5 trillion in financial losses because of cybercime attacks by 2024 (Juniper Research, 2019).

While the banking industry is among the greatest beneficiaries of the IT revolution and emerging technology (Goel, 2016), banks are also the most targeted for

cyberattacks. Banks and other financial institutions are attractive targets of cybercriminals because of their access to data and money (Perez & Suek, 2019). Smith et al. (2019) indicated that one of the first accounts of cybercrime occurred in the 1970s, involving a New York bank that suffered more than $2 million in fraud via computer. Lekha and Prakasam (2018) asserted that cybercrimes committed in banks include ATM card cloning, phishing, hacking, credit card scams, and money laundering. Hackers view these acts of cybercrime as an opportunity to gain high returns with low risk, often making profits by selling stolen information illegally (Smith et al., 2019). Hackers invade business servers by stealing personal information such as social security numbers, security questions, financial data, and home addresses (Hemphill & Longstreet, 2016).

The increase of organized, persistent, and modernized cybersecurity attacks on industries has created a challenge for businesses to stay protected (Ahmad et al., 2020). In 2018, the average cost of cybercrime incidents per organization increased by more than 1 million dollars, where the banking industry incurred the largest percentages of losses (2019). Many cases of cybercrime incidents are unreported, making it difficult to accurately estimate losses (Smith et al., 2019). According to the 2018 Ponemon report, the United States led worldwide in the highest number of data breaches, with an average cost of $7.91 million, followed by Canada at $4.74 million, and Germany with $4.67 million (Ponemon, 2018). Additionally, the associated cost to implement security automation averages $2.88 million and businesses that fail to implement security automation may risk incurring financial losses as high as $4.43 million (Ponemon, 2018).

Cyber Insurance and Cyber Talent

A new class of insurance known as cyber insurance began to emerge in the early 1990s (Erickson & Neilson, 2018). Cyber insurance is designed to mitigate losses from various types of cyber incidents, including data breaches, business interruption, and network damage (Department of Homeland Security, 2020). Franke (2017) reported cyber insurance as an approach to IT security which involves risk management and mandatory customer requirements. A robust cyber-security insurance market could help reduce the number of successful cyberattacks by promoting the adoption of preventative measures in return for more coverage and encouraging the implementation of best practices by basing premiums on insured levels of self-protection.

Cyber insurance is a policy derived from the origin of *errors and omissions insurance* designed to help businesses recover and mitigate risks from a cybersecurity breach or related event (Lindros & Tittel, 2016). Because of the many financial losses that banks were experiencing related to cyber deception and money transfer fraud; Grandpoint Bank created one of the first know cyber insurance group policy (Grandpoint Bank, 2016). Managing financial risks is as essential as managing security risks for IT businesses. Cyber insurance was created as a form of risk mitigation for companies to protect their assets from financial losses as result of the many cyberattacks (Heath, 2018; Talesh, 2018). According to Lindros and Tittel (2016), business leaders must decide which risks to accept, avoid, control, or transfer. Having cyber insurance provides a business with the ability to transfer some of the financial risks associated with a cyberattack (Bodin et al., 2018). More than one third of American companies have

incorporated some type of cyber insurance as part of their risk mitigation plans (Lindros & Tittel, 2016). Peters et al. (2018) indicated that cyber insurance premiums in 2015 amounted to $1.3 billion in the United States and continued to grow at an average of 10%-25% per year.

Cyber insurance policy coverage and premiums prices vary because of the uniqueness of the risks faced by each IT business and customization needed for each policy written (Peters et al., 2018). One policy may be written to cover insured losses for privacy liability, network security, intellectual property, and media breaches; while another may be written to cover insured losses for crisis management, business interruption, data asset protection, and cyber extortion (Peters et al., 2018). Despite the variations of each policy, when considering the term and pricing of a cyber insurance policy, four core determinants should be considered: the company size, type of data collected, method of storage, number of customers, and internet presence (Peters et al., 2018). Insurance companies expect an upward surge and project demand for cyber insurance premiums reaching $20 billion by the year 2025 (DiGrazia, 2018). The increase in insurance premiums is reflective of the continuous complexity of cyberattacks and IT systems (Marotta et al., 2017).

Carter (2016) predicted insurance premiums to continue to rise as cybercriminals were on target to collect $1 billion through cyber extortion. However, insurance premiums are used to cover the cost of the extortion payments, destroyed or disrupted services/assets, and ransom to release or transfer assets (Peters et al., 2018). Many IT businesses purchase cyber insurance policies that specifically cover breaches to mitigate

cyber extortion risks (Carter, 2016). Bodin et al. (2018) suggested that cyber insurance be used as a tool to reduce information security risk and should be included as a component of an organization's risk management program.

The damages of a cyber-security breach are far more extensive to a business than the financial losses initially seen. Arcuri et al. (2017) suggested cybersecurity breaches can harm the economy, including a decrease in stock value, decline in profits and revenues, and damaged company reputation. When customers think that their personal information and transactions are no longer confidential, they lose faith in the business (Smith et al., 2019). Cyber insurance can aid in mitigating loses and restoring customer confidence.

Many business leaders are challenged when making the financial decision to purchase cyber insurance or forgo the expense (Meland & Seehusen, 2018; Stephen, 2016). Raghavan (2018) reported that direct hits for cyber incidents could have a wide range of insured economic losses, ranging from $620 million to 8.1 billion. In 2014, the retail store Target experienced a data breach, costing Target between $450 million to $500 million in civil lawsuits, investigations, revenue loss, government fines, and computer network lawsuits (Hemphill & Longstreet, 2016). According to Raghavan (2018), as cybercrimes of this nature continue to increase, so will businesses demand for cyber insurance protection. Skeoch (2022) suggested implementing a modern cyber insurance policy that covers financial loses that occur from a cyber-attack along with those cost associated with hiring a computer forensic expert to help with analyzing the breach.

While cybercrime has created a financial crisis for many organizations, it has also created many employment opportunities in the field of cybersecurity (Cobb, 2018). The existing IT workforce is unable to meet the rising demand for qualified professionals with the needed cyber-security skills (Cabaj et al., 2018). As cybercriminals continue to grow in their sophistication of threats toward businesses and individuals, they have outpaced the pool of available cyber talent, widening the cybersecurity skills gap (Crumpler & Lewis, 2019).

The lack of qualified professionals with cybersecurity skills has become a hot topic in the IT industry (Furnell et al., 2017). Crumpler and Lewis (2019) stated that employers have a major need for cybersecurity professionals with the skills to design secure systems, identify vulnerabilities within the network, and create new defense tools. According to Blažič (2021), Cybersecurity Ventures a research company on global cyber statistics, predicted a shortage of 3.5 million cybersecurity jobs in 2021. The shortage of qualified cybersecurity professionals will present a problem for businesses with the requirement to develop a strong talent pool and viable cyber-security strategic plans.

Types of Cybercrime Attacks

Cybercriminals have numerous ways to interfere with business networks. As businesses and individuals increase their online presence by using the computer to complete transactions, the more opportunities there are for criminals to attack (Kumar & Carley, 2016). These attacks may take the form of a data breach or cyberattack, where both are unauthorized intrusions or attempts to invade a computer network (Romanosky, 2016). Sometime these unauthorized attempts may come from a company insider, who

might be an ex-employee or a disgruntled employee looking for revenge or some financial gain (Romanosky, 2016).

The type of cyberattack may vary depending on the specific line of business and the results that a cybercriminal hopes to achieve. For example, an attack called *zombie zero* has a specific design to attack logistics and shipping companies (Gliha, 2017). A denial of services attack is often targeted at banks, where the attack is directed toward security professionals, to insert malicious malware (Goel, 2016). If a criminal wished to request a ransom from a company, they may corrupt system files or prohibit access until the fulfillment of demands are made (Brewer, 2016).

A few of the most common methods of cyberattacks and threats are malware, phishing, spyware, denial of services, hacking, spamming, and credit card fraud (Goel, 2016; Kumar & Carley, 2016; Lekha & Prakasam, 2018). Guo et al. (2016) posited that malware corruption continues to cause the most significant financial losses worldwide and presents as a top security concern for businesses. Malware attacks alone, cost companies in the United States an average of $2.6 million dollars in 2018, an increase of more than 15% from 2017 (Bissell et al., 2019). According to International Business Machine (IBM) Security 2021 Cost of Data Breach Report, data breach costs rose from $3.86 million in 2020 to $4.24 million in 2021 (IBM, 2022). As a result of an increase in malware attacks, businesses need to ensure they have a strategic plan available with trained staff in place to keep their systems and networks safe (Simmonds, 2017).

Businesses consider malware attacks to be one of the most serious and common form cyberattacks (Russell, 2017). Companies globally report that malware attacks are

the leading cause of leaked confidential data (Iovan & Iovan, 2016). Malware is malicious software used to infect computers, tablets, or cell phones (Pascanu et al., 2015). The malicious software has the design to mislead users into clicking a link, thus giving the hacker access to either steal data or damage the network (Russell, 2017). The malware becomes injected into a system via a virus, botnet, worm, rootkit, spyware, adware, or trojan (Rudd et al., 2017).

Prayudi and Yusirwan (2015) defined a few common forms of malware. Prayudi and Yusirwan described a virus as malicious software designed to attack a computer system with excessive usage of memory, destroying data, and operating system. The botnet runs specific malicious commands, infecting a computer with malware, causing the computer to obey prompts as if instructed by a server (Paganini, 2020; Prayudi & Yusirwan, 2015). Rootkit hides malware so that the malware is undetected by antivirus software, while trojan is malicious software that installs itself and opens the gate for other hackers as described by Prayudi and Yusirwan. Downloader, a hacker installed program, allows the unauthorized download of additional data from a victim's computer (Catak et al., 2020; Prayudi & Yusirwan, 2015). Scareware, also known as leakware is malware used to scare victims into believing that their system has been infested or susceptible to sabotage; requesting the victim to pay a ransom for relief. (Kok et al., 2019).

Rudd et al. (2017) reported that advances in malware might allow malware to operate as a worm when propagating over a network, a virus when spreading over a host, and later transform into a rootkit, making the malware undiscoverable by intrusion detection software. Malware is also undetectable by antivirus software because of

analysis avoidance, longevity in the host, and fingerprinting (Prayudi & Yusirwan, 2015). Cook (2017) suggested a network infected by malware could impact thousands of devices before being discovered by the system owner. Prayudi and Yusirwan posited that malware is one of the most severe threats associated with cybersecurity.

Ransomware is a type of malware that prohibits access to files or corrupts an entire system until the hacker receives a reward (Iovan & Iovan, 2016). The malware encrypts files, backup drives, and other local drives and computers associated with the network, all unknown to the victim (FBI, 2020). Hackers then send a ransom demand message to release or return the hijacked system or data to its victim (Mohurle & Patil, 2017). Patyal et al. (2017) indicated that in a ransomware attack, victims make payments in the form of pre-paid credit cards or using bitcoin, both making it nearly impossible to trace back to the attacker (Aidan et al., 2017). In June of 2019, the University of California at San Francisco was attacked by a hacking group called Netwalker who demanded a ransom payment of $3 million in the form of bitcoin (Campean, 2019; Cook, 2022). According to the State of Ransomware 2022 report, the average ransomware payment in 2021 reached $812,000, which was approximately a 50% increase from 2020 (Jones, 2022).

Cyber-criminals began shifting their attacks from individuals to targeting businesses, which offer criminals the greatest in monetary rewards (Mansfield-Devine, 2016). Mansfield-Devine indicated that according to a 2016 trend micro report, 44% of businesses surveyed had at least one ransomware attack in the past two years. The attack and demand methods on IT businesses became more vicious and sophisticated over time.

Organized cybercriminals now use the latest in software and hardware technology, just like software developers use to implement their attacks (Monteith et al., 2021). Cybercriminals have advanced from infecting systems through malicious Uniform Resource Locators and spam mail to infiltrating servers directly or injecting malicious code on universal serial bus (USB) storage drives when targeting larger systems. The demand methods for ransom payments also became more sophisticated by using programs such as *jigsaw* – threat to delete data by the hour if not paid, and *surprise* – threat to increase the ransom amount if not paid by a specific time (Freedman, 2020).

Two of the most known infamous types of ransomware attacks are *wannacry* and *petya* (Javed Butt et al., 2019*)*. Although wannacry was the largest ransomware attack in 2017, petya first emerged in 2016, and its devious version occurred in June 2017 (Aidan et al., 2017). Petya destroys by corrupting the master boot record of a windows operating system, ultimately crashing the computer system. The damaging effects of petya are evident not only in the United States but also in other countries such as India, Germany, Brazil, and Russia. Although, businesses within the United States are still the primary targets.

On February 15, 2016, two separate ransomware incidents were ongoing, one on the East Coast and the other on the West Coast. Both IT departments had the challenge of making a decision that was best for their business. On the East coast, Horry County schools relented to the demands of the attacker and provided the ransom amount of $8,500 in bitcoins to regain access to their computer network (Patyal et al., 2017). On the West coast, Hollywood Presbyterian Medical Center paid a ransom of $17,000 to free its

system of ransomware infections (Patyal et al., 2017). Incidents of this nature are just a few reasons why IT business leaders seek strategies to prevent cybercrime attacks for their businesses.

According to Brewer (2016), there are five distinct phases of a targeted attack on businesses. Brewer suggested developing a ransomware defense system that requires an understanding of what happens in the five stages of a ransomware attack. In Phase 1, exploitation and infection, phishing emails and exploit kits are tools for attacking outdated software applications on computers. The targets of attack are Adobe flash and Internet explorer. Brewer indicated that the best way to counter the attack is to ensure that all software is current. In Phase 2, delivery and execution, persistent executable files of malware will attach to a user's profile. The defense is to know where to look and remove malicious malware (Brewer, 2016).

In Phase 3, back-up spoliation, shortly after delivery and execution, the backup files and folders are the next target for destruction. Once all backup files no longer exist or are invalid on the system, there is no recovery (Brewer, 2016). Phase 4, file encryption, after the removal of back-up files, encryption keys established on the local system become means to deliver specific instructions to the user (Brewer, 2016). The encryption methods all vary depending on which variant of the ransomware. Phase 5, user notification and cleanup, the demand instructions requesting payment appear to the user. After paying the ransom, the malware automatically removes itself from the victim's system without leaving forensic evidence (Brewer, 2016).

Other Methods of Cyberattacks

IT leaders must become informed of the current myriad of intrusion schemes to mitigate cybersecurity breaches and develop cybercrime prevention strategies for their businesses. Phishing, although one of the oldest techniques in a cyber criminal's arsenal, is also the most popular attack method and is on the rise (Binks, 2019). Phishing is just the first step to a more severe attack (Vincent, 2019), and the greatest cyber threat to businesses worldwide (Binks). Phishing is a type of online theft that deceives its victims through fraudulent emails or other communication methods, by making the communication appear to be official or from a trusted source (Mishra et al., 2018).

Recent trends showed an increasing number of phishing attacks on businesses, in which organizations are experiencing attacks daily and, in some cases, hourly (Boddy, 2018). According to Iovan and Iovan (2016), phishing attacks are number one in external attacks against businesses. Cybercriminals are specifically directing their phishing attacks, targeting finance, and accounting employees, along with those who manage business processes and IT security (Boddy, 2018). The losses in these attacks can be massive. For example, in 2014, a phishing attack cost BitPay $1.8 million in losses (Case & King, 2016). In 2015, the FBI also reported businesses losses of more than $214 million because of phishing attacks (Case & King, 2016).

IT business leaders need to understand how they become targets in a phishing cyberattack. Mishra et al. (2018) stated that the primary methods of phishing attacks used are deceptive phishing, pharming, sphere phishing, and whaling. Sphere phishing and whaling are the most popular type of phishing attacks and are used to specifically to

target leaders of a business or a specific group based upon the functions they perform within an organization (Binks, 2019; Mishra et al., 2018). An example of sphere phishing, also called Chief Executive Officer (CEO) fraud, is where attackers target a specific group or individual and make them think that the email is coming from the CEO of the company (Binks, 2019).

Binks (2019) reported that employees open 23% of phishing emails, making reducing human error a top priority. According to Vincent (2019), for IT businesses to better defend themselves, employees must first be aware of potential real-time attacks and who the attackers are. Vincent suggested that business leaders break the code of isolated defense and exchange information with their peers in the industry to combat the destructive power of phishing (Binks, 2019). Binks recommended company-wide education for employees as the most effective way to prepare for a phishing attack and to keep IT infrastructure safe.

DoS and DDoS attacks are some of the worst threats to a computer's network security (Khan et al., 2018). Cyber attackers use DoS or DDoS attacks to block communication channels between networks and tamper with the transmission of the data (Fei et al., 2021). According to Russell (2017), many IT businesses are primary targets of DDoS. Russell explained that this type of attack is activated by using botnets and other tools to overload servers with an abundance of internet traffic, such that the system is no longer accessible or crashes.

One example of how dangerous a DDoS attack can affect a business occurred in 2016, using the *mirai* botnet (Russell, 2017). The mirai botnet infects the Internet of

things (IoT) devices, later launched DDoS attacks on a plethora of other computers and businesses upon its release. Similarly, a research and education network crashed because of a DDoS attack when students purchased the malware from a website called booters, which impacted several schools (Santanna et al., 2015).

Cybercrime Prevention Strategies

Cybercrime occurs when someone infiltrates a computer system or network illegally, without permission from the system's owner (Saragih & Siahaan, 2016). Banham (2017) identified people as the weakest link in security protection, making people the first line of defense to cybercrime prevention. Campean (2019) suggested that experienced cyber thieves always target the end user as the entry point of a cyber-attack. As advances in technology have made systems more secure, attackers' resort to changing their method of attack to target humans (Holdsworth & Apeh, 2017). User awareness must strengthen, making employee information security training and education a requirement to help mitigate risks (Kim et al., 2020). According to Iovan and Iovan (2016), the two most significant areas of development for reducing cybersecurity risks are user awareness and education.

Human insight and expertise are just as important as technology when it comes to recognizing and responding to potential cyberattacks (James, 2018). Countering cybercrime attacks requires human intervention along with the ability to understand the attacker's mindset, which is a skill that cannot be duplicated entirely by non-humans (James, 2018). Employees must learn to recognize illegitimate phishing emails (Boddy, 2018). According to Heartfield and Loukas (2018), humans can act as sensors that detect

and report security breaches. In many cases, the human sensory of cyber threats is more accurate than any business security technology (Heartfield & Loukas, 2018).

Banks (2016) explained that leadership must first demonstrate human preventive actions. Banks asserted that in businesses with a healthy foundation, employees look to leadership to set the example of practicing cybersecurity safety. Erickson and Neilson (2018) supported this theory by suggesting that the C-suite own and embrace the risks associated with cybersecurity with the same level of importance as any other business risk. When leadership, the IT department, and fellow employees work together, they can manage and mitigate cyber threats more effectively.

Cyber Resilience

One premise for conducting research on cybercrime prevention strategies is for companies to become resilient and better prepared in the event of a cyberattack (Peter, 2017). Hawkins (2017) suggested that leaders incorporate the three Rs of cybersecurity—resistance, response, and recovery—to mitigate risks, limit the impact of an attack, and recover quickly. In other words, organizations equipped with the ability to prevent, detect, respond, and recover with little, or no damage are cyber resilient (Wilding, 2016). Wilding implied that company leaders, should be thinking outside-of-the-box from cyber-security to cyber resilience.

Businesses that prepare for cyberattacks by becoming cyber resilient, adopt a more holistic approach to cyber threats, preparing companies to maintain business operations despite adverse situations (Carias et al., 2020). According to Ledesma (2014), resilience is the ability to rebound from mishaps, affliction, and frustration, and is a

fundamental characteristic needed for effective leadership. Ledesma explained that recovery, durability, and thriving are also principles associated with resilience and describes a process that one facing an affliction will incur. How well business leaders navigate through the process of affliction will determine their level of resistance and then recovery time. According to Hawkins (2017), the most efficient form of resistance for an organization is to be prepared and having a strategic response plan in place in the event of a cyberattack.

Response Strategies

Despite the many cybercrime preventive measures that a company may employ, inevitably, a data breach may still occur. Business leaders are encouraged to develop resilience and to have a response strategy prepared (Gwebu et al., 2018; Wright, 2022). The objective of the cyber response plan is to lessen the damages incurred due to a cyber-attack (Phillips & Tanner, 2019). Russell (2017) asserted that all businesses, regardless of the sector or size, should prepare for a cybercrime attack, being proactive and not reactive. The proactive approach in cybercrime prevention for IT businesses requires having a solid plan in place and employees who are committed to carrying out the plan. According to Densham (2015), giving a designated employee an action plan in the event of an attack can significantly reduce the impact of the data breach.

Hawkins (2017) suggested developing a response plan in the resistance stage of a company's strategic planning, ensuring that all employees are aware of the steps to follow in the event of a cyberattack and that they follow proper communication channels in their response. Communication is a basic element of the response plan when an IT

system experience disruption. Hawkins purported that the response plan communication strategy should comprise of six primary elements: assess, locate, act, analyze, communicate, and collaborate. How quickly and efficiently an organization responds to an attack will determine the level of damage either suffered or deflected. Undoubtedly, strong communication skills and quick actions will become the drivers in how well a company recovers from a cyberattack.

The effects of a cyberattack impacts more than just the business and its employees, stakeholders, suppliers, and partners also suffer the attack. Hawkins (2017) advised maintaining levels of communication with all parties. Hawkins also recommended the installation of critical communication technology so that multiple platforms exist to distribute messages via social media, SMS, VoIP, mobile devices, and email. Businesses must ensure that platforms are multi-mode to allow for two-way communications, allowing IT engineers to respond to the source. Hawkins concluded that poor management in the response and recovery stage could cause the company to lose millions in revenue and customers.

In July 2016, President Obama established a cyber incident response plan that led to the development of Presidential Policy Directive 41, which defined the nationwide response to cyber incidents (The White House, 2013). The Presidential Policy Directive 41 was created to enhance policies previously in place to address cyberattacks so that both the private sector and the government would have a shared interest in protecting the nation against cyber incidents. The response plan included how the government prepares and recovers from colossal cyberattacks. Both the Department of Justice and the

Department of Homeland Security play vital roles for threat and asset response and recovery in significant cyber incidents (Department of Homeland Security, 2016; NIST, 2019).

Before the establishment of Presidential Policy Directive 41, Executive Order 13636 – improving *critical infrastructure cybersecurity* – came into existence in February 2013 (NIST, 2019). The objective of the order was to ensure that systems and assets vital to the United States would have a consistent and procedural approach for managing cyber-security risk, regardless of the company's size or threat exposure. Within the order, the cybersecurity framework featured, providing a set of common standards and guidelines to mitigate cyber-security risks and strengthen essential cybersecurity infrastructure. The core of the framework comprises four fundamental areas: functions, categories, subcategories, and informative references that addresses how to respond and recover against cyberattacks.

Insider Threats

A major problem for many businesses is insider threat (Le & Zincir-Heywood, 2018). In 2019, Securonix Insider Threat Survey reported that 73% of businesses confirmed that insider attacks have become more prevalent (Rodbert, 2020). Mazzarolo and Jurcut (2020), reported that the increased number of insidious damages committed by insiders, should serve as a warning to all cyber security personnel. Inside attackers are performed by individuals with authorized privileges such as business organizations and current working employees who are familiar with system policies and procedures (Suresh & Madhavu, 2022). More specifically, 63% of IT users/admins have been identified as

insiders that pose the greatest security threat to business (Schulze, 2018). The rise in insider cyber-crime activity has made addressing insider threats a top priority for providing greater protection of computer networks (Liu et al., 2018).

An inside attack can be carried out more easily because insiders have full access, privileges, and working knowledge to company assets and are able to launch attacks that appear like normal work activities (Gheyas & Abdallah, 2016). The inside attacker focuses on the destruction and compromising of confidential data or damaging critical network infrastructure. Insider attacks are normally attributed to employees, consultants, contractors, temporary workers, and other associated third-party personnel (Schultz, 2015). In conjunction, a collaborative attack between insiders and associated outsiders, can make it difficult to determine if the attack is internal or external.

Rodbert (2020) noted that with the rise in insider threats, companies must become more aware of the risks involved and prepare correctly to handle challenges developed by insiders. Oh et al. (2019), stated that insider detection depends heavily upon the function and purpose of the business. Unfortunately, unlike a robber or rapist who fit a certain profile, there is no unique profile that can be used to identify an insider who commits criminal crimes (Cole & Ring, 2005). Although, companies that have become serious about detecting insider threats, they realize that old methods for protecting confidential data and critical network assets no longer work (Cole & Ring, 2005).

Regrettably, only 60 percent of insider cybercriminal activity is detected (Le & Zincir-Heywood, 2018). Rodbert (2020) purported that senior leadership be committed and focused on circumventing insider activity across the business; in a manner such that

their actions and beliefs are disseminated throughout the rest of the organization. Another factor in insider detection and preventing insider sabotage is being able to identify the malicious insider type. Liu et al. (2018), believed that insiders who bring harm to businesses via the computer are labeled as masquerader, traitor, or unintentional perpetrator. Knowing each insider type, provides businesses with valuable knowledge in being able to track, detect, and possible prevent a system from being sabotaged by an insider.

Education and Training

Holdsworth and Apeh (2017) indicated that with the rapid increase of cybercrime, relying on and hoping that technology alone will keep systems secure no longer seems realistic. Instead, well-trained users aware of the current cyberculture must supplement the use of technology. Organizations are strongly encouraged to deploy education and employee awareness as a countermeasure to cyberattacks (Hart et al., 2020). According to Aldawood and Skinner (2018), businesses that adopt innovative IT security education programs might increase user awareness and significantly reduce the impact of cyberattacks. The vulnerabilities of humans require addressing weaknesses through awareness training and education (Holdsworth & Apeh, 2017). Companies that fail to educate their employees properly are putting their intellectual property, customers, stakeholders, and company reputation at risk.

The National Initiative for Cybersecurity Education (NICE) believes that through education, cyber risks are reduced, resulting in better security in cyberspace (Newhouse et al., 2017). By educating the public, cyber threats are recognized and avoided:

education helps IT professionals cope with the latest technology and prevention strategies; education prepares the workforce for the future. NICE is an initiative led by NIST in partnership with the private sector, the government, and academia to promote a robust platform for cybersecurity education and training to develop skilled cybersecurity professionals for the workforce (Newhouse et al., 2017).

Crumpler and Lewis (2019) revealed that as cyber threats continue to increase, businesses need to find qualified professionals with the necessary skills to protect their systems from cyberattacks. Crumpler and Lewis indicated that a workforce shortage exists for almost every position related to cyber-security. According to Crumpler and Lewis, businesses are in severe need for cybersecurity professionals that (a) create new defense tools, (b) detect vulnerabilities in the network and software, and (c) design secure systems. Employers are looking for employees with more technical skills and less of cybersecurity planners and compliance officers (Crumpler & Lewis, 2019).

To help combat the cybersecurity workforce gap, in 2009, NIST and leaders from the Department of Homeland Security (DHS) and the Department of Defense (DoD) developed the NICE cybersecurity workforce framework as a training resource and standard for developing, recruiting, and maintaining cybersecurity talent (Coulson et al., 2018; NIST, 2019). The framework is a resource highly recommended for IT professionals, students, or anyone who aspires to become proficient in cybersecurity.

Closing the cybersecurity gap is imperative and may be facilitated by allowing individuals to increase their cybersecurity skillset through education and training (Vogel, 2016).

Legal Aspects of Cybercrime

Law is a system that defines what can or cannot be done legally (Wilk, 2016). Any illegal or criminal activity committed with a computer as either an instrument or target is considered a cybercrime (Khimani & Parekh, 2017). As technology of the internet/intranet became more progressive so did crime on the network (Saragih & Siahaan, 2016). The increased devastation of cybercrime on businesses resulted in the subsequent passing of state and federal laws (Smith et al., 2019). More specifically, in 1984, Congress formulated the Computer Fraud and Abuse Act to address the threat of malicious code designed to destroy or damage computer networks (Congress, 2019; Duan, 2020).

It is paramount that IT professionals are aware that the legal aspects of cybercrime are just as important as understanding the technical details of cybersecurity (Erendor & Yildirim, 2022). Universities are advised to invite legal experts into the classroom to lecture on cybercrime reporting and cyberlaws (Mwiraria et al., 2022). IT professionals and students would benefit by developing more courses in ethics, law, and social issues as part of the computer science undergraduate curriculum. Although, cybercriminal activity continues to outpace legal legislation, policies, and academic literature (Phillips et al., 2022).

Corporate business leaders and IT officers have the responsibility to secure data as it relates to information technology (Trautman & Ormerod, 2017). Smedinghoff (2008) suggested that leaders and officers provide effective security procedures that maintain the integrity, confidentiality, and availability of corporate data. This

requirement to provide effective security is not just on one single source of obligations for corporate data security but a multitude of privacy laws, consumer protection laws, corporate protection laws, and data breach notification laws (Smedinghoff, 2015).

Business leaders must understand the legal requirements when developing cyber-security priorities (Deighton, 2015). Based on Deighton's research, risk mitigation plans, policies, and procedures must be in writing to coincide with the law effectively enforced. Trautman and Ormerod (2017) maintained that some electronic transaction laws require businesses to maintain fidelity, accuracy, and data integrity to meet the requirements of data security for electronic record keeping. Business leaders are challenged to have basic legal knowledge and seek legal advice when needed because cyber laws can be complex and change often (Wilk, 2016).

Conteh and Royer (2016) revealed that two reasons for the prevalence in cybercrime are the increase in opportunities over the Internet and the relatively low risk and safety for hackers. In cybercrime, the probability of arrest due from leaving DNA evidence, shoeprints, or footage from a security camera is relatively low. Thus, cybercriminals compare the low risks of detection with the many incentives and high returns and continue to commit these malicious acts of crime (Smith et al., 2019). Though having cyber laws in place is good, IT businesses have adequate protection when they have effective cybersecurity preventive strategies in place.

The Active Cyber Defense Act is a bill introduced to congress in 2019 to explain the prosecution of fraud and related criminal activity committed via computers and for persons defending against illegal acts of computer intrusion (Congress, 2019). Within the

bill, congress first acknowledges that cyber fraud and cyber-related computer crimes place the nation's security and economic strength at risk. The bill also states that citizens or businesses affected by such crimes should first report the infringement to law enforcement, followed by an update to their methods of defense. Finally, the purpose of the bill was to provide legal clarification of the techniques and tools likely used to overstep the boundaries of a computer network.

The only exception defined in the bill is for attribution technology. Attribution is the art of finding out who committed a computer crime and the method or technology used in identifying the felon (Rid & Buchanan, 2015). Data such as timestamps, usernames, Internet Protocol (IP) address, malware samples, log files and metadata gathered through forensic analysis are inclusive of attribution data. According to the active Cyber Defense Act, attribution technology refers to programs used by the defender to provide locations, attributional data, or the source of an intrusion (Graves, 2019). IT business leaders must be aware that attributional data may be legally confiscated as evidence to help prosecute cybercriminals.

On April 12, 2000, the Cybersecurity Information Act (H.R.4246) introduced to Congress was to encourage the secure disclosure and protected exchange of information about cybersecurity problems, solutions, test practices, test results, and related matters in connection with significant infrastructure problems (Congress, 2020). This act, otherwise known as the Cybersecurity Information Sharing Act of 2015, was voted into law in December 2015 (Kans, 2018). This act introduced several other cybersecurity-related bills that recently became law, such as HR3359 – Cybersecurity and Infrastructure

Security Agency Act of 2018, HR5515 – The John S. McCain National Defense Authorization Act for Fiscal Year 2019, and S.770 – NIST Small Business Cybersecurity Act (Congress, 2019; Kans, 2018).

The NIST Small Business Cybersecurity Act (S. 770) came into existence when President Donald Trump signed it into law on August 14, 2018 (Townsend, 2018). This law requires NIST to help small businesses reduce their cybersecurity concerns and risks by providing them with clear and precise resources that address their cyber needs. Small companies more often lack the resources, tools, and budget to manage cyber-security risks effectively (NIST, 2019). Therefore, congress gave NIST the responsibility to disseminate resources (NIST, 2019) and provide guidance for necessary security prevention and best practices needed to counter cyber threats (Townsend, 2018).

According to Saragih and Siahaan (2016), several strategies are crucial to repel cybercrime. Effective cybercrime prevention strategies must be in place to support the global economy and to ensure that individual assets and business assets remain secure (Cook, 2017). While many factors influence IT business leaders in what, how, and when to implement cybercrime prevention strategies, each business leader must determine what strategies must be in place and best serves their company. The literature review provides information that substantiates the need for IT businesses to implement cybercrime prevention strategies for the continued success of their business and the protection of customer, vendor, and stakeholder data.

Transition

Section 1 included a background introduction to the study, the problem statement, the purpose of researching this problem, the research method, and design. Other discussions in the section included the nature of the study, research question, interview questions, and the significance of the study. I also provided an in-depth review of professional and academic literature to explain the phenomenon of the impact of cybercrime activity on businesses. In Section 2, I restate the purpose statement and provide a detailed description of the role of the researcher, participants, data collection, data analysis, and verification of data reliability and validity. Section 3 includes the presentation of my findings and the results of the study after the analysis of data. Other components consist of my final recommendations on cybercrime prevention strategies for IT business leaders and conclusion.

Section 2: The Project

In this section, I restate the purpose statement of this study and elaborate on the main steps for conducting the research. This includes defining my role as the researcher, describing the participant selection process, and explaining the selected research method and design. Within this section, I discuss the process for data collection and data organization and describe the tools and procedures used in collecting the data. I also describe how the data captured from the research questions were analyzed, showing reliability and validity.

Purpose Statement

The purpose of this qualitative multiple case study was to explore effective cybercrime prevention strategies that IT business leaders use to protect their businesses from cyberattacks. The targeted population was comprised of IT business leaders of companies located in the Midlands region of South Carolina, who have implemented effective strategies that help protect their businesses from cyberattacks. Potential implications for positive social change include the potential for creating an environment wherein consumers are more confident in conducting business with IT companies, which may stimulate the economy by producing more jobs and building schools for the community.

Role of the Researcher

The role of a qualitative researcher is to act as the primary instrument to collect data and perform analysis of the data (Karagiozis, 2018). A part of this role is ensuring the collection of data is objective and without bias. My 20 years of experience working in

IT and the aviation industry relates to cybersecurity. Notwithstanding my related experience in cybersecurity and understanding the importance of avoiding cyberattacks, I did not have any personal relationship with any of the participants in the research.

Another part of my role as a researcher was to comply with ethical principles as noted in the Belmont Report. The Belmont Report, a standard for conducting research involving human subjects, has three principles: (a) respect for persons, (b) beneficence or ensuring minimal injury to human participants, and (c) justice (Friesen et al., 2017; Lantos, 2020). In compliance with the ethical principle of respect for persons, I was respectful of the participants and sought their consent on issues such as recording the interview. To ensure compliance with the principle of beneficence, I allowed participants to choose the location of the interviews. I did not force participation in the research. To ensure justice, I ensured that the selection of participants for the study occurred by a fair sampling method based on selection criteria.

Researchers mitigate biases by being mindful not to let personal beliefs, values, or behaviors influence research outcomes (Karagiozis, 2018). To ensure an objective data collection process, I followed an interview protocol (see Appendix A). Yeong et al. (2018) wrote that the key to obtaining quality interview data is having a reliable interview protocol. According to Castillo-Montoya (2016), an effective interview protocol comprises of four phases: (a) ensuring interview questions align with the general research question, (b) conducting inquiry-based conversations, (c) receiving feedback, and (d) piloting the interview. By using an interview protocol, I adequately addressed biases, conducted quality interviews, and received valuable feedback.

Participants

Participants were business leaders in the IT industry who provided relevant answers to the research question. One of the selection criteria was that participants were currently business leaders of companies that offer IT support with more than 150 employees. Participants were six IT professionals with responsibilities of overseeing and ensuring a secure IT network and infrastructure. Participants had two or more years of cybersecurity experience or training and had successfully implemented and used cybercrime prevention strategies.

Gaining access to participants is a process of finding and securing qualified participants for research (Peticca-Harris et al., 2016). Garcia et al. (2017) suggested that recruiting participants via personal referral is most successful. After obtaining approval from Walden University's Institutional Review Board, I viewed personal contacts and LinkedIn contacts to find qualified business leaders to take part in the interviews. By using my networking and communication skills, I gained access to willing participants.

According to Guillemin et al. (2018), trust is a significant factor in the success of participant research. Guillemin et al. (2016) revealed that establishing trust and rapport with participants is an interpersonal matter between participant and researcher. I expressed the importance of confidentiality and anonymity with my participants, which is an important principle in human research (Lancaster, 2017). I was honest and open with participants, revealing my personal reason for doing this research to establish a working relationship with participants.

Research Method and Design

In the following section, I present a description of the research method and research design for this study. A qualitative research method and muti-case design was appropriate for this study. I share the justification for the chosen research method and design, and I explain the relevance to answering the research question.

Research Method

I selected a qualitative approach to explore cybercrime prevention strategies used by IT business professionals to protect their businesses from cyberattacks. Qualitative research is research that produces findings not derived by statistical data or other quantifiable methods (Rahman, 2017). According to Holloway and Galvin (2017), the goal of qualitative research is to explore, understand, and describe the real-life experiences of the participants. The qualitative approach provided the opportunity for social inquiry, allowing people to interpret their experiences from the perspective of the world in which they live (Kruth, 2015; Rahman, 2017). I used the qualitative method to understand the phenomenon of cybercrime prevention strategies for data networks in real-life settings.

Cybercrime prevention is a phenomenon that can be researched from both a quantitative and qualitative perspective. In quantitative research, measurement of the phenomena is taken from the angle of brand awareness, penetration, and preferred products; this approach requires numbers and percentages within a given set of constraints (Barnham, 2015). Researchers have a narrow focus, searching for explanations and precise predictions and testing hypotheses with tight control (Holloway

& Galvin, 2017). Facts become evident by using a series of *what* questions (Yin, 2018). In contrast, qualitative research is relevant to gain an in-depth understanding of participant experiences, motivations, and behaviors (Queiros et al., 2017). Researchers assume a holistic and person-centered perspective (Holloway & Galvin, 2017). Deep probing occurs by asking *why* questions. Researchers seek to understand why participants behave or think the way they do. In comparing the two research methods, I determined the numerical analysis of quantitative research would not allow me to ask probing questions about participants' experiences of strategies used to combat cybercrime and effectively protect system networks.

Mixed-methods research involves using both quantitative and qualitative research. Mixed-methods research is the collection, analysis, and combination of qualitative and quantitative data (Guetterman et al., 2019). The sequencing of research elements must be clearly defined from both qualitative and quantitative research and is explicit for data triangulation (Denscombe, 2008; Taeuscher & Laudien, 2018). Researchers use mixed methods to give added value, despite the additional resources, time, and expertise required to perform a study (McKim, 2017). While mixed methods may have provided a more thorough understanding of a business problem, it was not relevant to my goal of understanding the strategies used to prevent IT business systems from being sabotaged by cybercriminals.

I concluded that a qualitative research method was best suited for this study. Qualitative research permits observation in a real-world context (Sawatsky et al., 2019), which in this case was the IT business environment of cybersecurity professionals. In

contrast, quantitative methods are most appropriate when factual data, supported by numbers and statistics, are necessary to answer the research question of a study (Hammarberg et al., 2016). In quantitative research, in-depth interviews provide a better understanding of lived experiences to address the research question (Macias & Contreras, 2019).

Research Design

I selected a multiple case study design to conduct my research. A case study is one of the most frequently used methodologies for qualitative research (Yazan, 2015). According to Kruth (2015), case studies are relevant to exploring a bounded system from several perspectives to gain detailed information on an event, series of events, or person. Lertora and Sullivan (2019) further defined a qualitative case study as a holistic analysis of a bounded phenomenon, such as a program, social unit, institution, or process. A multiple case study allows a researcher to create a more convincing argument with the collection of multiple forms of data (Gustafsson, 2017). Using a multiple case study approach may allow in-depth inquiry into the phenomenon of strategies that IT cybersecurity professionals use to protect businesses from cybercrime.

Kruth (2015) highlighted four other designs for quantitative research: narrative, phenomenology, ethnography, and grounded theory. The approach best suited for research will depend on the focus of the study and the results the researcher wants to achieve (Kruth, 2015). Considering my goal to gain an in-depth understanding of cybercrime strategies used from multiple perspectives, I elected to use a multiple case study design to gather data from experiences of IT professionals in daily real-life settings.

Prior to selecting a case study design for this qualitative research study, I evaluated other possible research designs. In a narrative approach, individuals or groups describe or explain past experiences primarily in the form of storytelling (Kruth, 2015). Clandinin et al. (2017) also suggested that narrative inquirers study individual stories through observation, listening, and living alongside them. The narrative approach is focused more on an individual's life experiences and would not provide data relative to answering the research question. Because storytelling involves more intense observation and is heavily dependent on a person's memory and not supporting data, the narrative design was not appropriate for my research.

The phenomenology approach focuses on the true "essence of an experience" (Kruth, 2015, p. 224). Phenomenological researchers explore the perceptions of individuals through their lived experiences by conducting in-depth interviews (Sorensen, 2018). I was not interested in the participants' perceptions of the phenomenon but in knowing the precise strategies used and outcomes of implementing such strategies; therefore, a phenomenology design would not have applied to my research.

The ethnographic researcher aims to understand behaviors and meanings associated with teams or groups (Sawatsky et al., 2019). According to Bryman and Bell (2015), the researcher becomes immersed in the culture as part of their investigation efforts. Such cultural immersion requires researchers to become engaged in the lives of the participants for an extended period (Marion et al., 2015). I was not interested in behaviors or the culture of a group. My goal was to obtain factual data of strategies used

by IT professionals to combat cybercrime. Therefore, an ethnographic design was not relevant to my study.

Population and Sampling

The population for this study was comprised of six experienced IT business professionals responsible for implementing cybersecurity practices that protect their business or other businesses from cybercrime. The selected IT professionals were from IT organizations located in the Midlands area of South Carolina, who had served in their roles for at least 2 years, were considered a leader, and have effectively implemented and practiced cybersecurity or cybercrime prevention strategies and techniques within their organization. The ideal participants selected were in positions of leadership such as chief information officer, chief information security officer, security engineer, cybersecurity managers security analyst, network engineer, and other team leaders.

I used purposive sampling, which is often used in qualitative research. Purposive sampling enables a researcher to conduct in-depth interviews, purposively selecting participants who can address specific research questions (Setia, 2016). Etikan et al. (2016) noted that purposive sampling is a deliberate choice by the researcher to select participants based on the qualities and skills they possess. Qualified participants are experienced and educated with the phenomenon (Barratt & Lenton, 2015; Etikan et al., 2016) that address cybercrime prevention strategies. Trochin (2006) defined purposively sampling as sampling with a purpose in mind; participants are selected from a pool of predefined groups. I chose a total of six participants from six IT companies.

Purposive sampling, also known as judgment sampling (Sharma, 2017), is a nonrandom process that does not require underlying theories or a specific number of participants (Tongco, 2007). Purposive sampling involves the selection of well-informed candidates experienced in the phenomenon under study (Serra et al., 2018). Hence, my goal was to select those participants who were not only experienced in the phenomenon but also eager to provide solutions to the business problem. Barratt and Lenton (2015) suggested that, in purposive sampling, a researcher should become knowledgeable with the field site and develop a rapport with the selected population. After selecting my interview candidates from colleague referrals and LinkedIn IT professionals, I introduced myself to the prospective candidates well in advance of conducting interviews for familiarization and rapport development.

Six participants who met the specified criteria from six IT companies were selected for interviews. A sample size with as few as six participants can be enough to achieve data saturation (Guest et al., 2006; Hennink et al., 2017). According to Bhardwaj (2019), when the number of people is small in population and the researcher has determined that the targeted population would fulfill the needs of the research question, this aligns with purposive sampling. Thus, I used the targeted sample size to achieve data saturation, in which no new themes emerged, which is a requirement in qualitative research to ensure data validity and accuracy.

In qualitative research, data saturation is a standard for quality research (Hancock et al., 2016) and is an integral part of this study. Saunders et al. (2018) described data saturation as the point in the data collection process, when no new information or themes

are evident, and findings become repetitive. Legard et al. (2003) and Saunders et al. (2018) warned against the premature ending of data collection. Experts advise continuing the probing process for a complete understanding of the participants' point of view and until confidence is gained about achieving saturation (Brawn & Clarke, 2019). When there are no additional similarities or apparent differences, the data collection process ends (Aldiabat & Le Navenec, 2018).

Data saturation is achievable during a single interview versus looking at the entire collection of interviews (Legard et al., 2003; Saunders et al., 2018). To achieve data saturation, interviews are conducted until it becomes apparent that no new information is being obtained and enough data has been collected to build a comprehensive and compelling theory (Morse, 1995). Data triangulation introduces trustworthiness and data credibility (Copes, 2014; Lemon & Hayes, 2020). Data triangulation was implemented into the study by using multiple data sources that included the interviews and supporting documents supplied by the participants achieving data saturation. Member checking also aids in creating trustworthiness and validity in qualitative research (Candela, 2019). Member checking was done by having participants verify the information that was collected from the interviews for data accuracy.

Ethical Research

Researchers have a responsibility to research ethically as required by the institutional review board (IRB) (Klitzman, 2019). The IRB is responsible for ensuring compliance with ethical standards of the University and U.S. federal regulations before recruiting participants or collecting data for research (DiGiacinto, 2019). According to

Lee (2018), any research that involves human subjects must follow a formal process and obtain ethics approval from a research ethics board. In this section, I discussed the informed consent process, disclosure of incentives, the process for participant withdrawal, a description of measures for ensuring the ethical protection of each participant, and data security. I followed the guidelines set by Walden University IRB and IRB approval number is 09-07-21-0477654.

Prior to performing data collection, researchers must obtain informed consent in writing per participant. According to Chiumento et al. (2016), the use of informed consent guides while conducting ethical research, help protect the rights of participants. Kadam (2017) suggested that valid informed consent requires giving participants enough information to make guided decisions about participating in the study. Having established a clear understanding of the study, each consenting participant completed an informed consent form located in Appendix B and duly signed, indicating voluntary participation in the study. Participants also received an explanation that there would be no incentives for participation in the study, and they could withdraw from the study at any time without penalty. I gave participants the option to withdraw from the study if needed. To withdraw, they needed to communicate their intention via a written letter, email, text, phone call or in person. The informed consent form and any data acquired from such withdrawing participants would have been destroyed within 24 hours of receiving their withdrawal notification, by shredding paper data and burning USB devices. There were no participants that withdrew from the study.

Researchers are encouraged to provide ethical protection for participants involved in the research. Resnik described the "*Belmont Report* as the most influential documents about research involving human subjects" (Resnik, 2018, p. 28). *The Belmont Report* specifies three basic principles for ethical guidance involving human subjects: (a) respect for persons, (b) beneficence, and (c) justice (Lantos, 2020). I implemented principles of ethical protection according to the *Belmont Report*, which acknowledges autonomy, considers the well-being of participants, and operate in fairness and equity (Adashi et al., 2018).

Additionally, to comply with ethical research and assure participant protection, I adhered to guidelines established by the National Institute of Health (NIH) as applicable. Emmanuel et al. (n. d.), shared that the NIH established guiding principles that preserve the integrity of science and protect volunteer patients before, during, and after clinical research. A few of those guiding principles include fair subject selection, favorable risk-benefit ration, independent review, and informed consent and respect for potential and enrolled subjects. These guiding principles helped to reinforce principles stated in the Belmont Report and met the requirements of Walden's IRB.

Data privacy and security are vital elements in practicing ethical research and a requirement of the IRB. To ensure the protection of participants' personally identifiable information was coded to uniquely represent each interviewee and their organization when documenting and organizing my data. Both participant and company name remained anonymous to ensure confidentiality. The use of special coding of numbers and letters to encrypt personal identification provide protection and privacy of participants

(Yin, 2018). Data captured was stored on a password protected USB drive. All written data is kept in a locked file drawer, along with the USB drive, and maintained for a minimum of five years. At the expiration of five years, the USB drive will be erased, and all raw data related to the study will be destroyed by burning and shredding.

Data Collection Instruments

In qualitative research, the researcher is the primary data collection instrument (Sarma, 2015; Yin, 2015, 2018). As the primary collection instrument, I collected data relative to the research question from each participant via semistructured interviews. Data collection in qualitative research often involves collecting date through detail interviews, audio recordings, note taking, and the researchers field notes in observation of the phenomenon (Renz et al., 2018). I elected to use a journal to take notes during the interviews to aid in clarification of what was being captured via audio. Each participant was given a clean page in the journal, documented with a special code to represent their file and protect their privacy. The permission to take notes was documented in the informed consent form.

One of the most popular and often used method of data collection in qualitative research is the semistructed interview (Evans & Lewis, 2018). The semistructed interviews were performed virtually using Zoom, an android cell phone and note takers journal. I collected supporting documents for review via email and downloaded data from the supplied government website NIST. Interview recordings were recorded via a Sony digital recorder, ICD-UX570 series and personal Hewlett Packard laptop, model IGS8VNGF.

In qualitative research, a well-defined interview protocol is essential in gathering quality data (Yeong et al., 2018). According to DeJonckheere and Vaughn (2019), a semistructured interview is comprised of a dialogue between the participant and researcher, using a flexible interview protocol as a guide to aid with followed up and additional questions. Roberts (2020) recommended using an interview protocol for structure and developing interview questions that answer the research question(s). I used an interview protocol as listed in (see Appendix A) and listed in the table of contents to facilitate the interview process.

In accordance with the interview protocol, each interview was allotted one hour, lasted between 45 and 60 minutes, and arranged on a date and time that was convenient for the participant. Interviews with key participants are a primary data source, for data collection (Hawkins, 2017). The semistructured interview allows participants the opportunity to freely express themselves, providing the researcher with rich and direct information (Li et al., 2019). Using open-ended questions allows the researcher to explore a topic in depth, explain causes of an observed phenomenon or better understand processes (Alishaikh et al., 2021; Weller et al., 2018). Ten open-ended questions were asked using the interview protocol to collect participant responses.

In qualitative research, the researcher is often the primary data collection instrument, lending to the propensity of researcher bias. According to Brear (2018), member checking is used to reduce researcher biases, enhance validity, and reveal a deeper understanding of the data collected. Member checking is the process of returning analyzed or interview data to participants for verification purposes (Birt et al., 2016;

Carlson, 2010). In performing the member checking process, each research participants were allowed to review my synthesis of their responses to the research questions and confirm accurate documentation of their intended message.

Data Collection Technique

In this qualitative multiple case study design, I interviewed six IT business leaders using semistructured interviews and an interview protocol (see Appendix A). Braaten et al. (2020) stated that well defined protocols aid in establishing consistency to research and builds quality. In case study research, the most common sources of evidence are non-participant observation, participant observation notes, file registration, physical artifacts, documents, and interviews (Fernandez et al., 2016; Yin, 2018). After obtaining consent from Walden's IRB, I started the process by contacting 13 participants that were acquired via references from other professional colleagues and LinkedIn. The initial form of contact was done via email and telephone. The pre-interview script (see Appendix C) guided the initial conversation. Six of the 13 contacted participants responded. After receiving participant agreement to participate in the study, the Informed Consent (see Appendix B) document was emailed to participants and returned via email. Upon receiving the returned informed consent form, the following steps were taken:

1. Each participant was emailed information about the study and, confidentiality, the interview process, and a copy of their consent form to participate.
2. A follow-up email was sent to establish a time and place to conduct the interview, stating the estimated time of the interview, and the tools that will be used to conduct the interview (see Appendix D).

3. On the interview day, each participant was reminded of the confidentiality agreement and their right to withdraw from the interview at any time (see Appendix A).
4. After each interview was completed, I explained how information would be transcribed, coded, transferred to NVivo and how anonymity is kept. Member checking was explained to ensure the accuracy of the answers.
5. The storage process of maintaining data for five years was explained and how the data is kept secured as well as discarded.
6. At the end of each interview, I thanked each participant for their time.

Interviews are a powerful method to gather information regarding a specific problem or subject from an interviewee (Fernandez et al., 2016). A semistructured approach allows an interviewer to gather significant experiences and opinions from participants regarding a subject matter (Naeem & Ozuem, 2021). The semistructured interview allows in-depth probing on specific topics, enabling the researcher to ask follow-up questions for clarity (Chu & Ke, 2017; Makhanya, 2019). Nyström et al., (2018) suggested that using semistructured interviews, provide researchers with greater flexibility to gain rich and insightful data. I used semistructured interviews that were recorded and took copious notes during the interview to explore strategies in cybercrime prevention for IT businesses.

As the primary data collector, in addition to conducting interviews, I performed document reviews of the supporting documents from the company relative to cybercrime prevention and network security. According to Wei et al. (2018), company documents

provide deep learning into the phenomenon being explored. Participants in the study supplied relevant NIST and DoD documents that met industry standards, which provided guidelines and procedures for integrating security measures. Document reviews provide information for triangulation that enriches the research (Noble & Heale, 2019). Exploring supporting documents provided by the participants via email and company websites, provided additional information on the techniques and strategies being used by IT business leaders to help mitigate cyberattacks.

There are several advantages and disadvantages associated with the preferred method of data collection. The advantage of the document review is the supporting data that is provided for information collected via other methods (Yin, 2018). Whereas the disadvantage is the limited accessibility for document reviews (Creswell & Poth, 2018; Yin, 2018). According to Morse (2015), the advantage of audio recordings allows the researcher the opportunity to listen to the interview multiple times during playback to gain greater clarity and understanding of the participants' responses. One disadvantage to the researcher, may be finding a quiet place, free from noises to complete audio recordings (Creswell & Poth, 2018). This disadvantage may be mitigated because many employees have the option to work from home, providing another location more conducive for interviewing. An advantage of the semistructured interview is the flexibility given to the researcher to ask deepening questions to gain greater clarity (Fernandez et al., 2016). A disadvantage associated with the semistructured interview is the associated extended time required in comparison to unstructured interviews

(Fernandez et al., 2016). By using the interview protocol script and being time conscious, I mitigated the disadvantage of extended time.

Enhanced reliability and validity of data is a required element in the data collection process, achievable via member checking. Simpson and Quigley (2016) noted member checking as a best practice to establish trustworthiness in quantitative research. Member checking provides an opportunity for participants of the study to verify the contents of the data that was provided by the review of transcripts or data interpretation (Carlson, 2010; Simpson & Quigley, 2016). When performing the member checking process, a final draft of the edited interview was returned to each research participant by email to confirm the accuracy of the captured responses and ideas. Participants were given seven days to respond with feedback and corrections. Three of the participants provided feedback which included name corrections, clarification, or additional resources. Transcripts were updated to reflect the corrections and documents reviewed to support information previously given to complete final analysis. If no additional feedback was given, the participant was contacted a second time to ensure that no additional updates were needed. Candela (2019) suggested that member checking can be helpful in maintaining validity and an opportunity for participant reflection.

Qualitative researchers may elect to perform a trial run of the interview and data collection process in preparation for the main study. Gallego-Jimenez et al. (2018), revealed that pilot studies in case study research may check the viability of the researcher's methodology and provide an opportunity to perform adjustments before beginning the study. Pilot studies are used to test the relativeness of interview questions,

aid the researcher in developing interview skills, and building rapport with the participants (Doody & Doody, 2015; Majid et al., 2017). A pilot study was not performed.

Data Organization Technique

Every researcher has a style for organizing their research. Qualitative researchers collect data in a myriad of forms: paperwork, spreadsheets, video recordings, surveys, webpages, pre-structured data, and more (Kuckartz & Radiker, 2019). I elected to organize and keep track of data and personal notes by using a journal. Each audio recording was transcribed by Happy Scribe and uploaded to a Word document and labeled using a unique set of codes. The transcripts were labeled using a 12-digit generated code, comprised of 3 company initials, 3 random digits, 3 digits that signify the day of week and 3 random digits that represent analysis software. For example, MAX456TUENVI, would represent the interviewee from Maximus corporation, 456 is a random selection of numbers, TUE is Tuesday from the day of the week and NVI represents NVivo software.

I used thematic analysis to analyze, organize, and report themes observed from within the transcription data (Nowell et al., 2017). To further organize and analyze the data, the data collected was transferred to a computer-aided qualitative data analysis software (CAQDAS). All audio recordings, notes documented, and WORD files were transferred and saved on a password protected USB drive. To adhere to Walden's University policy, all data will remain in a secured file cabinet until after five years, then discarded by burning USB devices and shredding paper data.

Data Analysis

According to Yin (2015), data analysis is the classification, testing, and arranging of evidence to draw empirically based results. Data analysis involves the processing of all data collected by the researcher during the data collection phase. Chowdhury (2015) described qualitative data analysis as coding, cataloging, and sorting of qualitative data that may either strengthen or weaken the reliability or robustness of the research. One approach to qualitative data analysis is the method for describing and interpreting participants' views, such as content and thematic analysis (Smith & Firth, 2011). Thematic analysis is a technique used to identify patterns and themes within qualitative data as described by Maguire and Delahunt (2017). NVivo software provides thematic analysis by categorizing statements according to themes and codes (Sezgin et al., 2019).

The results of thematic analysis have served as a foundation for understanding deeper forms of specialized analysis (Lester et al., 2020). I analyzed themes and patterns to give meaning to the information drawn from the participant interviews, notes taken, and documentation reviewed using NVivo software and the conceptual frameworks of GST and theory of transformational leadership.

To mitigate the chance of researcher bias, while demonstrating validity and reliability of the data, triangulation was used. The basic concept of triangulation is the use of two or more data sources to provide a more reliable outcome versus using a single source (Ashour, 2018). The technique of methodological triangulation is the use of multiple methods to investigate the same phenomenon as explained by Ashour. Interview transcripts, personal notes, published documents, and member checking were used to

explore the subject of IT cybercrime prevention strategies. Joslin and Muller (2016) revealed that methodological triangulation enhances the validity of a researcher's study and strengthens the results (Bekhet & Zauszniewski, 2012).

The data analysis process began with a review of the data captured via audio recording and the notes taken from each interview question per participant. The notes taken during the interviews were used to clarify words, ensure correct spellings, give context to questions, and collaborate with the transcribed data. Supporting documents that were emailed or retrieved from supplied websites along with government documents supplied from member checking, were reviewed as support for strategies used in cybercrime prevention. I synthesized interview responses, coded, and labeled, and organized the data for input into the analysis software. The use of CAQDAS tools enhances the researcher's ability to obtain and analyze qualitative data (Prabowo, 2020). In qualitative research, a researcher may choose from a variety of CAQDAS programs such as NVivo, ATLAS.ti, MAXqda, and webQDA (Reis et al., 2016). Each program has its own unique set of features that makes more favorable over the other. For example, NVivo software has a feature for importing and storing qualitative data such as audio recordings, transcriptions, and other relevant documentation (Paulus et al., 2017). NVivo provides tools for handling rich data and categorizing and coding data (Bazeley & Richards, 2000). For this study, NVivo 12 was used to derive themes from answering the interview questions.

Results of the analysis process was done by an inductive approach. In inductive reasoning, the researcher may engage in several research activities such as code

development, discovering and seeing patterns and identifying themes (O'Kane et al., 2021). I analyzed the data using GST and transformational leadership as the framework to help me understand the meaning of the data collected. Using the GST framework to examine the themes and patterns generated via NVivo 12, aided in understanding how different teams worked together to develop strategies used by IT leaders to defend their network. By looking at the collected data through the lens of transformational leadership, I understood how leaders in the IT industry empower and aspire team members to implement effective cybersecurity strategies within their organizations.

Reliability and Validity

Reliability

Reliability and validity are two techniques used for soundness and completeness in qualitative research. The assessment of the quality of a qualitative study depends on ensuring reliability, validity, and generalizability (Leung, 2015; Noble & Smith, 2015). Reliability is the evaluation of research for the replicability of processes and outcomes (Leung, 2015). In qualitative research, the core of reliability lies in the adequacy of the data, demonstrating consistent support of the researcher's analysis across all respondents (Spiers et al., 2018). The more times the duplication of a study's finding remains constant, the more its reliability (Cypress, 2017).

The quality of a study exists to establish credibility, transferability, confirmability, and dependability (Amankwaa, 2016; Shenton, 2004). *Dependability* in qualitative research is evident when findings are repeatable and consistent (Amankwaa, 2016; Noble & Smith, 2015). Qualitative researchers demonstrate dependability by

employing techniques such as transcript reviews, pilot testing, triangulation, and member checking (Creswell & Guetterman, 2018). Qualitative researchers may use at least two of the techniques in each study for validation purposes (Creswell & Poth, 2018). For this study, I implemented triangulation and member checking.

According to Creswell and Baez (2021), detailed notes and transcription of the audiotape will enhance reliability. I used a journal to take notes and had the audio recording of the interview questions transcribed by Happy Scribe transcription service. I kept track of my journal notes and made additional notes on the hard copies of the transripts and questions for reliability. An interview protocol was used for each participant interview to ensure a uniform procedure, eliminating inconsistencies in mitigating researcher bias. All questions were listed in the interview protocol. Member checking, also known as *writ large* in qualitative research, provides participants with the opportunity to review the analyzed data, interpretations, and conclusions for accuracy and trustworthiness (Creswell & Poth, 2018).

Validity

Validity in qualitative research refers to the suitability of the methods, tools, and data analysis, which produces positive research outcomes (Leung, 2015). Cypress (2017) stated that validity in research relates to how accurate and truthful the results of the data analysis are. Validity in data, assists in providing an accurate account of participant experiences within and beyond a defined context (Spiers et al., 2018). In the 1980s, Guba and Lincoln determined that the trustworthiness of qualitative research was achievable through reliability, validity, and generalizability replacing dependability, transferability,

and credibility (Morse, 2015; Noble & Smith, 2015). Strategies such as member checking, triangulation, and peer debriefings help achieve credibility and establish internal validity (Morse, 2015). Cypress (2017) indicated that member checking, through constant checking of interpretations and representation of the data with respondents, also demonstrates credibility. Triangulation establishes validation using two or more methods or datasets to explain a question or expand understanding (Morse, 2015). Both member checking and document review was used for triangulation purposes, which also served to validate my study.

Transferability and confirmability are two additional criteria for demonstrating trustworthiness in qualitative research. *Transferability* shows that the findings in a study are applicable in other contexts (Amankwaa, 2016). Shenton (2004) indicated that transferability exits when the results of the research, although unique, apply to a larger population. Transferability, also known as "reader generalizability," where research strategies are applicable to other settings, goals, and practices (Maxwell, 2021). The use of the interview protocol and detailed notes taken in the journal, that was used in this proposed study will aid in demonstrating transferability.

Confirmability refers to objectivity in a study (Shenton, 2004). The focus of confirmability is to ensure that the findings of the research have no researcher bias, personal interest, or motivation, but reflects the genuine responses of the participants (Amankwaa, 2016). The effects of researcher biases are reduced through triangulation and the managed predispositions of the researcher (Abdalla et al., 2018; Shenton, 2004).

Cuthbert and Moules (2014) stated that demonstrating credibility, transferability, and dependability are antecedents of confirmability.

Data saturation is significant in establishing rigor in all qualitative research (Guest et al., 2020). Saunders et al. (2018) highlighted that saturation occurs when no new information or themes emerge from data collection, and findings become redundant. Data obtained from interviews can be entered into a saturation grid which is a simple report that tracks the occurrence of each theme (Fofana et al., 2020). I used semistructured interviews and continued to collect data until no new themes were apparent.

Transition and Summary

In Section 2, I restated the purpose statement, described my role as the researcher and primary data collector, expounded on research method and design, population and sampling, data collection methods, and steps to ensure reliability and validity of the data. In Section 3 of the study, I provide a brief introduction and then the findings of the study were presented as applicable to professional practice and implication for social change. Further recommendations for the future and suggestions for further research are presented later in the study. The conclusion of the study includes my reflections, final analysis, and experiences as a researcher.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The objective of this qualitative multiple case study was to explore effective cybercrime prevention strategies that IT business leaders use to protect their businesses from cyberattacks. I interviewed six participants who worked in IT organizations located in the Midlands area of South Carolina. All participants were strong advocates for adopting cybercrime prevention strategies to protect system networks from cyberattacks. Using NVivo software to analyze the data collected, I discovered three primary themes: (a) cybercrime prevention strategy; (b) cybersecurity awareness, training, and education; and (c) effective leadership. Additionally, three subthemes were revealed: (a) incident response plans, (b) policies and procedures, and (c) third-party vendors. I used the theory of transformational leadership and GST as the conceptual framework for the study in which I confirmed the connection with cybercrime prevention strategies. In this section of the study, I provide a presentation of the findings, application to professional practice, implications for social change, recommendations for action, recommendations for future research, reflections, and a conclusion.

Presentation of the Findings

The central research question for the study was: What effective cybercrime prevention strategies do IT business leaders use to protect their businesses from cyberattacks? Using purposeful sampling, six participants who met the selection criteria participated in individual interviews. Each participant was emailed an informed consent form and agreed to an audio recorded phone interview that would last between 45 and 60

minutes. I used multiple open-ended semistructured interview questions and took handwritten notes in a journal for each question. Supporting documents mentioned in the interviews were supplied through public resources or provided directly through email and were subsequently reviewed as part of the analysis. Microsoft Word was used to transfer each transcription text file into a Word document. I then proofread the Word document for corrections and imported the information into NVivo. QSR NVivo Plus 12 was used to organize and analyze data into themes. According to Roberts et al. (2019), thematic analysis is content analysis of non-numerical data, in which themes and codes that emerge from the data become categories for analysis. The results of the thematic analysis allowed me to connect many of the responses to the literature reviewed, as related to the research question.

In Table 1, a summary of participant demographic information is listed. The six participants interviewed had a minimum of 2 years of experience in their leadership roles and a maximum of 15 years. Participant experiences included owner and president of a cybersecurity company, security team lead, blue team member lead, chief information security officer, and chief security officer. I assigned pseudonyms to the participants starting with Participant 1 as PA1 for the first business to Participant 6 as PA6 for the sixth individual interviewed.

Table 1

Participant Demographics

Participant	Age	Years in leadership	Years in the IT field
PA1	45	10	22
PA2	36	8	15
PA3	55	5	20
PA4	49	5	10
PA5	56	18	25
PA6	36	2	10

To derive the themes, I did a top-21-word search query of key words referenced during the interview. I then used NVivo's auto theme query to identify themes relative to the research (see Appendix E for query results and theme identification per participant responses). From the data analysis of the queries, three themes emerged: (a) cybercrime prevention strategy; (b) cybersecurity awareness, training, and education; and (c) effective leadership. I identified three subthemes: (a) incident response plans, (b) policies and procedures, and (c) third-party vendors.

Theme 1: Cybercrime Prevention Strategy

The first theme identified in this study was cybercrime prevention strategy. The relevant subthemes under cybercrime prevention strategies are incident response plans, policies and procedures, and third-party vendors. The primary objective of this study was to identify cybercrime prevention strategies used by leaders in IT businesses to protect

their companies' network. The rapid increase in cybercrime activity has caused businesses to put into practice more effective strategies of cybercrime prevention (Shah et al., 2019). All participants recognized the need for IT businesses to become more aggressive in their approach to keep their networks secure against cyberattacks and provided strategies they have implemented.

Each participant provided one or more strategy for cybercrime prevention. PA2 stated, "I think the most important strategy is a cybercrime defense strategy." To effectively counter vicious attacks against company networks, organization are urged to enhance their cyber defense capabilities (Ho & Gross, 2021). In cyber defense, the role of the defender is to identify potential flaws within an organizational system, determine how to exploit it, and then figure out how to make those changes to remediate or close the gaps as part of the organization's defense (Ge et al., 2021). PA1 stated that understanding the environment is the first step in building a strong defense strategy. In terms of cyber defense, PA4 stated, "You have to be proactive. You cannot sit around and wait for an attack." IT business leaders and their employees must be in a posture to defend themselves, prepared for an attack.

PA2 explained that a cybercrime defense must be based on defense in depth, which aligns with Borky and Bradley's (2018) theology of a layer defense approach. The strategy of cyber defense also resonates with Mutlak (2017) who suggested multiple layers of risk defense for effective risk management in cybersecurity. The advancement and variety of cyberattacks requires multiple levels of security to be combined at different levels, with intrusion detection systems listed as the first line of defense in

detecting unauthorized entries (Rubio et al., 2019). PA1 was also in agreement with this philosophy, stating, “I have to visibly see everything that is going on within my environment.” PA1 shared that tools are integrated into the system to monitor the traffic and detect unlawful entries. Both PA6 and PA4 cited intrusion detection systems tools in their environments to monitor traffic. PA4 indicated, “Monitoring the network is so important that they have engineers whose primary job is to monitor the network traffic all day.”

While advancement in technology has created new sophisticated tools that IT personnel can incorporate into their networks as part of their cybersecurity prevention plan, they should not neglect proven traditional methods used to protect their systems. PA1 and PA6 strongly advised using a virtual private network (VPN) to secure one’s privacy while online. PA2 indicated that they always make employees log in via VPN working from home or offsite. PA4 also encouraged using VPN; they suggested that work be conducted on business-issued laptops only, rather than using personal computers. PA3 underscored the importance of using remote security access tokens that use two-factor authentication to gain access to their business server. PA3 stated, “We have to use the [remote security access] token.” PA5 stressed using multifactor authentication for offsite work when working with vendors and using laptops. Participants also shared the importance of creating difficult passwords and changing them frequently. Keeping antivirus software up-to-date and installing firewalls are simple strategies IT business leaders should enforce in their business units to help with cybercrime prevention. A cybercrime prevention strategy can be comprised of several

subcomponents. Analysis of the NVivo data revealed three subthemes used most often by the participants: incident response plans, policies and procedures, and third-party vendors.

Incident Response Plans

Incident response plans emerged from the data as a subtheme for cybercrime prevention strategies used by IT business leaders. An incident response team follows a written set of procedures or plans used to respond, detect, and limit the effects of a cyberattack (Toth, 2017). Having an incident response team in place with a designated leader and plan is a top priority for organizations to effectively manage a cyberattack (Wertheim, 2019). This concept is in alignment with the findings of Angafor et al. (2020), who argued the importance of training cybersecurity incident response teams for proper cybersecurity management. Several participants strongly supported having an updated incident response plan in place to ensure employees know what to do in the event of an attack, shortening recovery time. PA6 shared that recovery plans should include having an updated phone list including personal cellphone numbers to call when a breach has been detected. PA1 stated, “So basically, we map out any particular security incidents that may happen and try to have a plan on how we would address them.” PA3 proclaimed that every area has a designated set of disaster recovery plans that include their cyber incident response plans. PA4 stated, “Once we are aware of the attack, everyone must be cooperative. We then follow an incident response plan, which is part of our security protocol, where everyone is assigned a particular task.”

One of the most renowned frameworks defining the standard of incident response life cycle was developed by NIST (Schlette et al., 2021). The incident response lifecycle is comprised of four criteria: (a) preparation, (b) detection and analysis, (c) containment, and (d) eradication and recovery (Toth, 2017). The participants provided NIST and DoD documents that I reviewed that corroborated with the information shared during the interviews. PA3 shared that once they have been made aware of a cyber breach, the security team is alerted, if not already informed, to begin the next course of action. PA1 indicated the use of forensics tools for digital analysis in the event of a breach, which aligns with Phase 2 of the incident response lifecycle.

Incident response teams are a precise example of how individual elements function together to fulfill the objective of an organization. In teamwork, every member of the organization contributes to overall goals of the organization (Kumari & Majumder, 2021). The structure of teamwork is breaking the workload into smaller pieces of work for everyone to have an assignment (Alarafat & Doblas, 2021). According to Phipps (2019), GST and the study of wholes and wholeness are viewed not as separate parts but observed as a whole. Each member of the response team is given an assignment to ensure that attacks are identified quickly and resolved, which aligns with the theory of GST.

Participant responses aligned with Lekota and Coetzee's (2019) view that organizations within the government and private sector realize the need for cybersecurity incident response teams to effectively manage cyber threats to critical networks. The cybersecurity incident response team or security team is made up of several fundamental positions to appropriately respond to a cyber event when the role of leadership is of

utmost importance. Moore (2022) explained that an incident response team may consist of a team leader, lead investigator, communications lead, documentation and timeline lead, and a legal representative. PA1, whose has served in the lead role of a cybersecurity incident response team, stated, “I must keep abreast of everything going on in the environment”; PA1 indicated they have made some tough decisions for the good of the company. PA4 also shared that, as a leader, they challenge employees by questioning them and asking them to solve problems. PA4 stated, “I question them to see if they can come up with the right solution versus asking me to resolve a problem; they can resolve themselves.” The participant responses aligned with the transformational leader, as noted by Karacu et al. (2014), who possesses characteristics of decisiveness, self-confidence, and intellectual stimulation. Such a leader must be competent and an effective communicator.

Policies and Procedures

Four participants indicated that the use of policies and procedures was essential to help combat and manage cyber threats. The aim of IT security/cybersecurity policies and procedures is to have well-documented instructions that provide direction to help an organization manage and mitigate cybersecurity risks (Mishra et al., 2021). Some of the procedures and policies mentioned were those that the organization follows from a national level as well as those developed internally by their IT business units. The goal of network security policies is to implement strategies that address security threats, mitigate IT risks, and define steps to recovery when a network is compromised by an attack (Salo et al., 2018). PA1 stated, “One of the first things we actually do is, when we come into

your environment, we start building out plans and policies because without policy, there is no security." PA6 also affirmed that their organization follows a set of procedures for handling security-related incidents and those procedures are often updated immediately after an incident has occurred to stay current. PA3 reported that their organization adheres to multiple policies and procedures to enforce security and ensure that new team members have well-documented instructions.

The national policies and procedures referenced by participants under NIST control are: (a) SP 800-53, (b) SP 800-54, (c) Federal Information Processing Standards 140, and (d) A10 Network Application Delivery Control. I reviewed these government standard documents used by participants to help develop and strengthen the cybercrime prevention strategies that IT business leaders implement. PA3 stated, "We rely on government standards under NIST control" and shared a copy of the security technical implementation guide, A10 Network ADC Application Layer Gateway, as one of the procedures used by their organization. PA2 shared that they developed their own data loss prevention procedure and strictly adhere to NIST industry standard policies SP 800-53 and SP 800-54. PA6 also reported that their organization follows the federal information processing standards, which is a U.S. government security standard for various data and computer systems.

Third-Party Vendors

Third-Party Vendors were revealed as a second sub-theme of cybercrime prevention strategies. All participants listed some vendor, commercial off-the-shelf product or business partnership that was used as part of their strategy to help keep their

networks secure or to restore operations quickly after an attack. Many IT businesses rely upon third-party vendors that utilize modern technology and cyber tools to assist them in daily operations (Reed & Scott, 2018). Third party vendors help to alleviate some of the responsibility and workload that would normally be the responsibility of the business.

The forward-thinking IT business leader recognizes the need to incorporate outside resources, seeking to leverage sophisticated tools and subject matter experts possessed by vendors (Campbell, 2018). PA5 discussed advising businesses to seek outside subject matter experts that would better serve their needs, if in house talent was not available. PA5 stated that some companies try using the same IT security employee to do cybersecurity work that they may not necessarily be skilled in, when it would be best to hire an outside source, pay a little more, and have better expert coverage. PA3 also agreed with the use of third-party vendors, stating that they use vendors often to perform certain types of specialized security services.

DeFord (2022) recommended having a retainer with a reputable cybersecurity company, that guarantees quick response time in the event of a cyber-attack. An effective cybercrime prevention strategy includes having quick access to resources as soon as an incident is discovered which is supported by DeFord, who stated that speed is the most important factor in the new era of cybersecurity. PA1 shared that part of his strategy was to put a company on a retainer, specifically to handle the analysis after a cyber-attack or data breach has occurred. PA1 explained, that obtaining a retainer is hiring a company whose job is to be on call to analyze the data files and better understand the nature of the breach. PA6 confirmed that their organizations use the support of a triage team to quickly

access the problem and recover from an attack. The triage team is composed of a subject matter expert in security and may include an outside resource. Wertheim (2019) argued that effectively managing a cyber-attack requires planning, preparation, and readiness which includes having a cybersecurity retainer agreement in place with a company that specializes in responding to cyber breaches.

The findings revealed that several IT business leaders included cyber insurance as a supporting element in their cybercrime prevention strategy. Participants 1, 2, 4, and 5 indicated they employed cyber insurance as part of their strategy to protect their business. Cyber insurance allows businesses to pass on some of the financial losses incurred, because of a cyber incident to a third-party (Xu & Hua, 2019), enabling them to focus on recovering more quickly. PA1 stated, “Then there is cyber insurance.” Implying that once their top two strategies are in place, cyber insurance is added as a third layer of protection. PA2 stated, “The biggest plan that we have is we carry cyber insurance.” PA4 also stated, “It is becoming very important to carry some form of cyber insurance.” PA5 further added that they were a strong advocate for cyber insurance, stating that some IT businesses, especially smaller companies, struggle with knowing if it worth the expense of purchasing cyber insurance. PA5 advices leadership to factor in cyber insurance as budgeted expense because the damages incurred as a result of not having insurance could far exceed the cost of adding it to the budget.

All participants mentioned the importance of education and training as part of their strategy to prevent cybercrime; often using outside sources or partner collaborations to support this endeavor. PA1 and PA2 both indicated their companies’ used SANS as a

resource to conduct annual training. PA2 stated, “One of my favorite strategies, one that I have deployed in different scenarios is using a provider called SANS.” PA5 indicated that they recommend to smaller IT businesses that they hire a vendor to come in and do training periodically.

To implement cyber-crime prevention strategies effectively, requires strong leadership, knowledgeable talent in a unified team, and a plethora of other resources. Many IT businesses contract third-party vendors to perform a variety of tasks, taking advantage of sophisticated cyber tools and skills that they don’t possess internally. Some of the additional third-party resources mentioned by the participants to help defend their networks were training vendors, cloud resources, and suppliers of tools such as VPN, Load Balancer, and Solar Winds.

The increased need to defend business infrastructures, continues to require more complex tools and often outside resources. According to the philosophy of GST, each IT organization is a system, including any outside vendors that the primary organization interacts with to implement cybercrime prevention strategies. Phipps (2019) shared that Ludwig Von Bertalanffy explored wholes and wholeness by investigating a phenomenon as a whole and observing the relationship between the parts. GST supports how relationships and the interactions between third-party vendors and IT organizations work together to solve complex issues for a common good of protecting the business network.

Theme 2: Cybersecurity Awareness, Training and Education

Cybersecurity awareness begins with leadership and must transcend downstream to every employee for IT businesses to effectively protect their network. The large

number of cyber-attacks and security breaches, costing companies millions of dollars has created a greater need for cybersecurity awareness. Cybersecurity awareness involves knowing the necessary requirements to protect your business information (Clark, 2020) and the steps needed to recover from an attack. Unfortunately, more attention has been given to how to respond to a cyber-attack after the incident, while the concern for cybersecurity and cybercrime prevention has lacked the attention it deserves (De Bruijn & Janssen, 2017).

A second theme that emerged from the interviews was that IT business leaders and employees be educated, trained, and aware of current trends in cybersecurity and cyber-attacks. An awareness in the cybersecurity phenomenon is not automatically generated but must be created within organizations. Increasing cybersecurity awareness among leadership to improve the management of threats and digital literacy is deemed as a priority of importance (Cirnu et al., 2018; Smith, 2019). Considering the rapid spread of cyberattacks on businesses worldwide, it is important that training and education become a priority and are addressed in a timely manner (Beuran et al., 2018).

In cybersecurity, Straub (2020) suggested that the first line of defense is the employee. Investing in your employee's education and training for cybersecurity awareness and the latest in technology, is your best defensive tactic in the war on cybercrime. According to a poll from 2018, more than 30% of chief cyber security officers interviewed, believed that their highest priority is to invest in employee security education and training first over other defense methods (Reeves et al., 2021). PA5 shared a similar belief stating, "The employee must be the 1st line of defense." PA5 believed that

constant training is necessary to keep employees aware of malware tactics and learn new strategies of cyber defense.

All participants were strong advocates for training and education, which aids in achieving greater cybersecurity awareness. According to Ho and Gross (2021), organizational cybersecurity awareness requires technically savvy cybersecurity professionals that are current in cyber defense knowledge and have a keen awareness of system breaking techniques. Creating an environment of awareness and educating employees on various types of online threats is a necessary component of a business cybersecurity strategy plan (Bada & Nurse, 2019). PA2 believed in doing annual trainings as one strategy in cybersecurity awareness. PA2 acknowledged, "We reuse the DoD publicly available cyber awareness training." I reviewed data that was available on the DoD website, which provides annual training via the Defense Information Systems Agency (DISA). PA3 noted that one method of staying aware and keeping current is for employees to attend conferences, workshops, and educational classes. PA3 also mentioned the use of DISA for training and staying current in cybersecurity procedures. DISA provides cyber and security related news, events, training, and media sources. A review of these resources provided a holistic look at cyber prevention tools that are available for training and education, which is in alignment with the holistic view of GST.

The findings from the study on using cybersecurity awareness, training, and education to prevent cybercrime, substantiate the findings of (Borky and Bradley, 2018) as an effective preventive technique to improve human vulnerabilities. The need for greater cyber security awareness, education, and training has become a national mandate

such that NIST developed the National Initiative for Cybersecurity Education. PA2 stated, “I’ve deployed different strategies using the provider SANS, that provides security awareness training.” PA5 recommended doing simulated cyber-attacks and random phishing exercises. PA5 suggested using the vendor KnowBe4, that provides internet security awareness training to help build a culture of security awareness.

Participant responses revealed that education and training added value to the organization and was a strong component of their strategic plan in cybercrime prevention. Employees that were given cyber awareness, education, and training on the job, were found to be more competent in detecting phishing scams and other security violations than those that had only received formal training (Reeves et al., 2021). Training in cybercrime prevention skills must continue beyond formal education as skills are developed and sharpened as part of continuous education and on-the-job training. PA5 reported that continuous education and training of cybersecurity scams and being able to identify phishing tactics, are imperative to circumvent and properly respond to a cyber-attack. PA1 suggested taking SANS courses and becoming certified in cybersecurity techniques. PA1 stated, “I like to recommend people take SANS courses, and try to get yourself certified, because getting certified empowers you and says what you are able to do.” PA2 also recommended using SANS as an educational provider for security training.

Participants 3 and 6 reported using compliance training as part of their annual required training. PA3 stated, “A portion of compliance training is related to cyber prevention.” PA3 stated that 10 hours of training is mandatory for every employee, then they have electives that they must take that relate specifically to their jobs in security.

PA6 indicated that their training departments conduct monthly training. PA6 stated, "These trainings help to identify these security threats. So, when an employee sees it, they know how to take the proper steps or procedures to handle the security threat."

Cybersecurity awareness, training and education are separate functions, yet closely linked together, to enhance the skills of cyber professionals. A principle of GST places emphasis on organizations as systems with an inflow and outflow that impacts the elements of the system (Von Bertalanffy, 2008). Through the lens of GST, training and education contribute to greater cybersecurity awareness, and greater awareness leads to the development of better training and educational tools. Responses from the participants indicated that IT business leaders are proponents for growth and increase in cybersecurity awareness, training, and education which are in alignment with GST and principles of the transformational leader.

Theme 3: Effective Leadership

Effective leadership is the third theme that emerged from this study. This theme represents the participants acknowledgement of the importance of their role as a leader, influencer, and the significance of safeguarding their business to ensure the success of their company. A business success in cybercrime prevention is heavily dependent upon the ideas and actions of its leadership. Senior executives have the power to influence and make important cybersecurity decisions that impact the culture of their organization (Parker et al., 2017). A company's leadership team is expected to make critical decisions in the event of a cyber-attack (Cleveland & Cleveland, 2018). Leaders that develop and

implement effective leadership styles, improve the overall performance, and job satisfaction for employees (Fahlevi et al., 2019).

Leaders of organization in the cybersecurity environment should be prepared to receive a call in the middle of the night regarding a cyber-attack (Cleveland & Cleveland, 2018). PA5 indicated that part of their training includes doing mock training drills when employees least expect them. PA5 also expressed incorporating mock attacks for employees that work at home. The mock attacks provided employees with an opportunity to learn what to do, should they ever experience a data breach while working at home or offsite. PA5 stated, “My job is to ensure that you are not caught with your pants down and don’t know what to do.”

One indicator of a business success is effective leadership and ineffective leadership is often a strong contributor to a business failure (Nyide, 2020). The effectiveness of leadership within a business is evaluated on how well employees understand what is expected of them and perform in terms of achieving company objectives successfully (Ali & Anwar, 2021; Smith 2021). The theme of effective leadership is supported by (Lehto & Limnéll, 2021), who suggested that effective leadership in cybersecurity must be strategic in identifying a response model and crisis management. PA5 stated that “As leaders we must have employees ready, not if a crisis occurs but when a crisis or attack occurs.”

Good communication is a basic skill of an effective leader that is needed in preparing a team for cybercrime prevention. Clear communication is important in an ever-changing world, in which cybersecurity is very dynamic. Leaders with good

communication skills help employees understand organizational goals, motivates them to support changes and fulfill the companies' mission (Cook, 2017). PA1 expressed the importance of making sure they have communicated to employees what their job is. PA1 stated, "Your job is to basically protect the company in case something happens." PA6 shared that they stress "communicate, collaborate, and confirm." Implying that there are different styles of communication and in some instances, you need to collaborate with others to ensure the message is clear. PA6 also stated that an employee should confirm that the message they are trying to convey is understood, by double checking to confirm. PA4 shared that it is important to effectively communicate the vision to the team and let them know the value they bring to the team in seeing the vision develop and come into fruition. PA4 stated, "I think you let employees know that they are valuable and bring something to the table. Then you get employee buy-in." PA3 viewed communication from a different perspective. PA3 believed in creating an environment where employees would feel comfortable about sharing anything with them. PA3 stated, "I encourage the open-door policy and I encouraged them to bring in their creative ideas."

The participant responses validated characteristics aligned with the concepts of transformational leadership; idealized influence, inspirational motivation, intellectual stimulation, and empowerment. PA2 stated that as a leader, they adapt according to the personality of the employee. PA2 recognizes that not all employees are alike, thus they lead from an individual perspective versus from a group. Recognizing the uniqueness of each individual employee is in alignment with the transformational leadership trait of 'individual consideration. PA1 indicated that they challenge their employees to prove that

they can perform certain tasks. PA1 stated, “I allow them to be great”, giving them the opportunity to show what they do best. This is a technique of intellectual stimulation which is also aligns with traits of the transformational leader.

Looking through the lens of GST, Mutlak (2017) recommended that every employee must be concerned about cyber security risks, starting with executive leaders of the company. Mutlak’s statement implies that every business unit, lower-level managers, and each individual employee in the organization, is responsible for all cyber risks. The responses from the participants are inclusive of everyone working together and align with Von Bertalanffy’s GST.

Applications to Professional Practice

The objective of this study was to reveal and discuss cybercrime prevention strategies that IT business leaders use to protect company assets from cyber-attacks. The study’s findings show how various strategies are employed by IT cybersecurity and network security leaders to safeguard their company networks from cyber criminals. The challenge to protect company assets has grown into a nationwide problem and multimillion dollar business. The methods that cybercriminals use to attack systems have become more sophisticated and damaging, thus requiring IT businesses to become more advanced in their strategies of protection. To respond effectively to a cyber-attack requires leadership awareness and a set of tested procedures for immediate response and solutions (Cleveland & Cleveland, 2018).

Based upon the findings in this study, successful IT business leaders should be aware of the evolving schemes of cybercriminals and proactively implement necessary

strategies to prevent or curtail the damaging effects of a cyberattack. The results of this study may help IT business leaders and their employees implement more effective cybercrime prevention strategies that will thwart the plans of cyber-criminals. The study revealed three major themes: cybercrime prevention strategy, cybersecurity awareness, training and education, and effective leadership. The three subthemes revealed were incident response plans, policies and procedures, and third-party vendors. Each theme presented vital information that IT businesses leaders may use to develop new cybercrime prevention strategies or enhance those strategies currently implemented by their organization.

Businesses as well as individuals are invoking extreme precautions, to secure their physical properties to prevent losses by installing security cameras, hiring on site security, and now the installation of doorbell security cameras. Many businesses, especially IT businesses have developed a sense of urgency to not only protect their tangible assets but also their digital assets. In 2021, the state of South Carolina incurred financial losses of $42 million because of cybercrime activity (McCreless, 2022). To aid in building a strong fortress against the attacks of cyber criminals, having a defined set of strategies provides a plan for protecting a company's infrastructure. Within those strategies, policies and procedures, including incident response plans, give clear directions for employees to follow in the event of an attack. Many companies are not equipped with cybersecurity talent, thus using third-party vendors are a viable option to ensure IT businesses have the necessary tools and skillset to help keep their networks secure and mitigate losses in the event of an attack. Acquiring cyber insurance helps to

alleviate some of those financial losses that may occur if their networks are breached. Finally effective leadership is essential for creating a culture that emphasizes cybersecurity awareness, training, education; and embrace those strategies needed for protecting the business network. IT business leaders that are inspired by the findings of the study and properly integrate these strategies may reduce financial losses in the event of an attack, bring antiquated strategies up-to-date, and aid in sustainability of their business.

Implications for Social Change

The implication for social change because of this study may positively impact communities, organizations, cultures, and institutions. IT business leaders that incorporate effective cybercrime prevention strategies that protect their systems in the event of an attack; has the potential to positively influence social change among many arenas. Businesses may safely expand in the community, bringing more jobs into the area, building better schools, and stimulate the local economy. Consumers are more willing to do business with businesses that they trust and feel that their personal identifiable information is being protected. Shareholders are more confident when they know that the businesses that they have invested with are applying the most current and advanced techniques to mitigate cyber risks.

Recommendations for Action

The threat of cyber-attacks continues to increase daily across the global. This is a phenomenon that will not be managed effectively without a set of proven strategies. The objective of this study was to discover those strategies that would aid IT business leaders

in protecting their systems from the attacks of cybercriminals. IT business leaders are encouraged to monitor their systems security and implement cybersecurity plans that are solid on defense (Teymourlouei & Harris, 2019). The strategies revealed in this study contribute to the body of knowledge in cybersecurity and are beneficial to IT leaders that desire to implement more effective cybercrime prevention strategies for their organizations.

Based on the findings, the first recommendation is for IT business leaders to develop a solid cybercrime prevention strategy. Creating a written strategy for swift implementation is the first weapon for safeguarding a network. The participants expressed the importance of having an incident response plan in addition to having policies and procedures in place. Policies and procedures are routine guidelines that are followed for safe cybersecurity practices such as two-factor authentication, changing passwords as recommended, ensuring that anti-virus software is up-to-date and only using work issued computers to perform their jobs. Should an attack occur, personnel will then follow an incident response plan to quickly resume operations and help mitigate losses. The strategy should also include partnerships with third-party vendors. Third-party vendors may comprise of subject matter experts on a retainer, hiring organizations that specialize in training or establishing a partnership with a cybersecurity insurance company.

The second recommendation is for greater cybersecurity awareness, training, and education. The constant changes in technology and the digital economy have required IT leaders to stay abreast of current trends or become less relative and financially at risk. IT

business leaders must continue to create a culture of awareness with education and training. Investing in employee education is imperative for a leader's strategic plan. One participant indicated that staying current meant attending outside trainings and conferences to learn what others are doing in the same industry to become more educated in cyberspace technology and trends. IT organizations should continue to enforce mandatory training and education, encouraging employees to become certified in a cybersecurity skillset when possible.

The final recommendation is for IT business leaders to embrace and practice effective leadership skills. The transformational leader is first known to lead by example. Employees, people in general are more motivated by what they see you do than by what they hear you say. I encourage IT leaders to be authentic and excited to embrace new ideas and technology in cybersecurity that may also inspire employees to embrace and adopt new concepts. IT leaders should also recognize the individualized efforts of every employee, applying a method of motivation that speaks to their heart and intellect, that will inspire them to embrace those cybersecurity prevention strategies that have been laid out for the organization.

These recommendations are first addressed to IT business leaders within the organization: chief information security officer, security management, and technical leadership. Every employee has an important role to ensure that the company's network is secure and should highly consider these results. The recommendations from the results of the study may add to the body of knowledge for cybersecurity, aid in developing future course material or serve as a basis for further research. I will also share the results of the

study with the participants of the study. I personally intend to use this study as a baseline for further research for publication, speaking engagements, and providing insight to my non-profit organization.

Recommendations for Further Research

The focus of this study was limited to IT businesses in the Midlands area of South Carolina. I would recommend exploring this topic across other geographical areas; locations that are known for their advancements in technology such as Silicon Valley in California or The Research Triangle Park in North Carolina. These two regions of the United States are known for leading the industry in innovation and technology development. Exploring this phenomenon of cybercrime prevention in regions that are more technologically advance could provide greater insight on tools and strategies that may help IT business leaders develop better strategies.

I limited the experience of the IT business leaders to a minimum of two years in their leadership role, which I had one participant that met that criterion. Further studies may include IT business leaders with five or more years of leadership experience in cybersecurity or security. Employees with longer tenure in their respective IT leadership roles may have more in depth experiences to share regarding the phenomenon. My final recommendation is to include IT business employees that may not necessarily have been in a leadership role per title but has experienced several cyberattacks within their business and has experience on how to navigate a cyberattack.

Reflections

The decision to pursue my Doctorate in Business Administration did not require a lot of convincing because it was always a dream that was in my heart. The decision to remain in the program and preserve required me to reach deep within to truly understand my 'why' for pursuing this goal. I knew it had to be bigger than just putting another degree on my wall for status or moving up the ranks in my career. This journey of perseverance was bigger than me. This goal incorporated leaving a legacy and the role of influence that I would have in the lives of others with big dreams.

My first preconceived idea was that if I had the intellect and was willing to study hard, I could master this program within a few years and be done. I was very wrong. After the second residency, I quickly learned that I was in great error and that my writings would be scrutinized at a much higher level of professionalism. Doing research took on a totally different meaning from the research that I had done in the past in academia and in the corporate environment. Pursuing this doctoral degree not only advanced my writing and critical thinking skills, but I developed patience, perseverance, and learned the significance of constructive criticism.

Despite my background in IT, I had no preconceived notions about the research topic of cybercrime prevention in IT businesses. I was open to learn from the participants who were experts in the field of cybersecurity and cyber defense. I was grateful and excited at the same time about the information that I was learning, and about the possible opportunities that may be available to me in my future. The themes that were revealed in the study were an indication of the different avenues that one could pursue for further

education or career options in the field cybersecurity. The conversations with the participants clearly represented a group of people that were excited about their work, who also recognized how important their jobs were in helping to keep their systems secure. This study helped me to better understand why I am fascinated with IT work and the solutions it provides to businesses and everyday users of technology.

Conclusion

The notorious attacks of cyber criminals on businesses infrastructures show no signs of relenting. In fact, their methods of attack have become more frequent, sophisticated, and costly. IT business leaders and their teams are faced with a tremendous task, to ensure that their networks are protected from the attacks of cybercriminals. The findings in this study may aid IT business leaders with solutions to help combat the problem of cybercrime and mitigate those risks associated with cyber-attacks. The recommended actions for IT business leaders were to implement cyber-crime prevention strategies that incorporates an incident response plan, detailed policies and procedures, and to hire third-party vendors and experts as needed for insurance or training. IT business leaders would also benefit from continued cybersecurity awareness, training, and education programs for employees. IT business leaders are encouraged to practice effective leadership skills that would engage and motivate employees to take ownership in the implementation of effective cybersecurity prevention strategies. The need for cybersecurity professionals and cybercrime prevention is a fast-growing phenomenon. Further research should include, using a larger sample size, leaders with five or more years of experience and doing research with IT businesses in parts of the country that are

more technologically advanced in research, which may yield additional strategies in cybercrime prevention for IT businesses.

References

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

Abdul, H. B., Sajjad, N. K., Siti, M. A., & Yasir, H. M. (2019). Transformational leadership style, followership, and factors of employees' reactions towards organizational change. *Journal of Asia Business Studies, 13*(2), 181–209. https://doi.org/10.1108/JABS-03-2018-0083

Adashi, E. Y., Walters, L. B., & Menikoff, J. A. (2018). The Belmont report at 40: Reckoning with time. *American Journal of Public Health, 108*(1), 1345–1348. https://doi.org/10.2105/AJPH.2018.304580

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. (2020). Situation awareness in incident response: An in-depth case study and process model. *ICIS 2020 Proceedings*, 1. https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/1

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017). Comprehensive survey on Petya ransomware attack. *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*. https://doi.org/10.1109/ICNGCIS.2017.30

AlArafat, M., & Doblas, M. (2022). Impact of effective teamwork on employee performance: The case of the telecommunication companies in the kingdom of

Bahrain. *iKSP Journal of Innovative Writings*, *2*(2), 07-19. https://iksp.org/journals/index.php/ijiw/article/view/71

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, Wollongong, NSW, 62–68. https://doi.org/10.1109/TALE.2018.8615162

Aldiabat, K. M., & Le Navenec, C. L. (2018). Data saturation: The mysterious step in grounded theory methodology. *The Qualitative Report, 23*(1), 245–261. https://doi.org/10.46743/2160-3715/2018.2994

Ali, B. J., & Anwar, G. (2021). Administrative crisis: The role of effective leadership styles in crisis management. *Ali, BJ, & Anwar, G. (2021). Administrative Crisis: The Role of Effective Leadership Styles in Crisis Management. International Journal of Advanced Engineering, Management and Science, 7*(6), 31–41. https://doi.org/10.22161/ijaems.76.4

Alishaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organization. *Computer & Security, 100*, 102090. https://doi.org/10.1016/j.cose.2020.102090

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23*(3), 121–127.

Amiri, I. S., & Soltanian, M. R. K. (2015). *Theoretical and experimental methods for defending against DDoS attacks*. Syngress

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Cyber security skills gap: Using tabletop exercises to solve the CSSG crisis, serious games. *Security and Privacy, 3*(6), 117–131 https://doi.org/10.1002/spy2.126

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How does cybercrime affect firms? The effect of the information security breaches on stock returns. Paper presented at the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy. https://ceur-ws.org/Vol-1816/paper-18.pdf

Argan, M., Özgen, C., Kaya, S., Argan, M. T., & Demirbas, M. (2022). Collecting memories in away games: The effects of team identification, community identification, and away game involvement. *Trends in Psychology.* https://doi.org/10.1007/s43076-022-00150-1

Ashour, M. L. (2018). Triangulation as a powerful methodological research technique in technology-based services. *Business & Management Studies: An International Journal*, *6*(1), 193–208. https://doi.org/10.15295/bmij.v6i1.209

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3) 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Banham, R. (2017). *Cybersecurity threat proliferating for midsize and smaller businesses*. https://www.journalofaccountancy.com/content/dam/jofa/issues/2017/jul/cyber-july-2017.pdf

Banks, N. (2016). Practice what you preach. *Computer Fraud & Security, 2016*(4), 5–8.

https://doi.org/10.1016/S1361-3723(16)30035-5

Barnham, C. (2015). Quantitative and qualitative research: Perceptual foundations. *International Journal of Market Research, 57*(6), 837–854. https://doi.org/10.2501/IJMR-2015-070

Barratt, M. J., & Lenton, S. (2015). Representativeness of online purposive sampling with Australian cannabis cultivators. *International Journal of Drug Policy, 26*(3), 323–326. https://doi.org/10.1016/j.drugpo.2014.10.007

Baskarada, S. (2014). Qualitative case studies guidelines. *The Qualitative Report, 19*(40), 1-25. https://doi.org/10.46743/2160-3715/2014.1008

Bazeley, R., & Richards, L. (2000). *The NVIVO Qualitative Project Book.* Sage.

Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Journal of Nurse Researcher, 20*(2). 40-43. https://doi.org/10.7748/nr2012.11.20.2.40.c9442

Beuran, R., Pham, C., Tang, D., Chinen, K. I., Tan, Y., & Shinoda, Y. (2018). Cybersecurity education and training support system: CyRIS. *IEICE TRANSACTIONS on Information and Systems, 101*(3), 740-749. https://doi.org/10.1587/transinf.2017EDP7207

Bhardwaj, P. (2019). Types of sampling in research. *Journal of the Practice of Cardiovascular Sciences,* 5, 157- 163. https://doi.org/10.4103/jpcs.jpcs_62_19

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security 19*(5), 200-312.

https://doi.org/10.1108/09685221111188593

Binks, A. (2019). The art of phishing: past, present, and future. *Computer Fraud & Security*, *2019*(4), 9–11. https://doi.org/10.1016/S1361-3723(19)30040-5

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802–1811. https://doi.org/10.1177/1049732316654870

Bissell, K., LaSallem, R. M., & Cin, P. D. (2019). The cost of cybercrime Ninth annual cost of cyber crime study. *Accenturesecurity*. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training, Technology in Society, 67. https://doi.org/10.1016/j.techsoc.2021.101769

Boddy, M. (2018). Phishing 2.0: the new evolution in cybercrime. *Computer Fraud & Security*, *2018*(11), 8–10. https://doi.org/10.1016/S1361-3723(18)30108-8

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(1), 527-544. https://doi.org.10.106/j.jaccpubpol.2018.10.004

Borky, J. M., & Bradley, T. H. (2018). Protecting information with cybersecurity. In *Effective Model-Based Systems Engineering* 345-404. https://doi.org/10.1007/978-3-319-95669-5_10

Braaten, B., Kramer, E., Kaifez, R., & Dringenberg, E. (2020). Accessing complex

constructs: Refining an interview protocol," *2020 IEEE Frontiers in Education Conference (FIE)*, 1-3. https://doi.org/10.1109/FIE44824.2020.9274260

Brawn, V., & Clarke, V. (2019). To saturate or not to saturate, questioning data saturation as a useful concept for thematic analysis and sample size-size rationales. *Qualitative Research in Sport, Exercise and Health, 13*(2). https://doi.org/10.1080/2159676X.2019.1704846

Brear, M. (2018). Process and outcome of a recursive, dialogic member checking approach: A project ethnography. *Qualitative Health Research*, *29*(7), 944-057. https://doi.org/10.1177/1049732318812448

Brewer, R. (2016). Ransomware attacks: detection, prevention, and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1

Bronkhorst, B., Steijn, B., & Vermeeren, B. (2015). Transformational leadership, goal setting, and work motivation: The case of a Dutch municipality. *Review of Public Personnel Administration*, XX(X), 1-22. https://doi:101177/0734371X13515486

Brown, M., Brown, R. S., & Nandedkar, A. (2019). Transformational leadership theory and exploring the perceptions of diversity management in higher education. *Journal of Higher Education Theory and Practice*, *19*(7). https://doi.org/10.33423/jhetp.v19i7.2527

Bryman, A., & Bell, E. (2015). *Business research methods* (4th ed). Oxford University Press.

Busse, C., Kach, A. P., & Wagner, S. M. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them.

Organizational Research Methods, 20(4), 574-609. https://doi.org/10.1177/1094428116641191

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security, 75*, 24-35. https://doi.org/10.1016/j.cose.2018.01.015.

Campean, S. (2019). The human factor at the center of a cyber security culture. *International Journal of Information Security & Cybercrime*, *8*(1), 51–58. https://doi.org/10.19107/ijisc.2019.01.07

Candela, A. G. (2019). Exploring the function of member checking. *The Qualitative Report*, *24*(3), 619-628. https://doi.org/10.46743/2160-3715/2019.3726

Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs, *IEEE Access*, vol. 8, pp. 174200-174221, 2020, DOI: 10.1109/ACCESS.2020.3026063

Carlson, J. (2010). Avoiding traps in member checking. *The Qualitative Report 15*(5), 1102-1113. https://doi.org/10.46743/2160-3715/2010.1332

Carter, J. S. (2016). Pay up or else: the ins and outs of cyber extortion insurance coverage. *Journal of Risk Management, 63*(10), 32. https://go.galegroup.com/ps/anonymous?id=GALE%7CA473942509&sid=googleScholar

Case, C. J., & King, D. L. (2016). Phishing: Are undergraduates at risk and prepared? *Issues in Information Systems*, *17*(1), 80-88. https://iacis.org/iis/2016/1_iis_2016_80-88.pdf

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811–831. https://doi.org/10.46743/2160-3715/2016.2337

Catak, F. O., Yazı A. F, Elezaj O, Ahmed J. (2020). Deep learning based sequential model for malware analysis using windows exe API calls. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.285

Chang, Y.-Y., Chang, C.-Y., & Chen, C.-W. (2017). Transformational leadership and corporate entrepreneurship: Cross-level mediation moderation evidence, *Leadership & Organization Development Journal*, *38*(6), 812-833. https://doi.org/10.1108/LODJ-10-2015-0219

Chattopadhyay, L., Wang, L., & Tan, Y. (2018). Scenario-Based insider threat detection from cyber activities. *IEEE Transactions on Computational Social Systems*, *5*(3) 660-675. https://doi.org/10.1109/TCSS.2018.2857473

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems*, *33*(3), 163–182. https://doi.org/10.2308/isys-52410

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2016). Ethical challenges to research in post‐conflict settings. *Developing World Bioeth*, *16*, 15-28. https://doi.org/10.1111/dewb.12076

Chowdhury, M. F. (2015). Coding, sorting, and sifting of qualitative data analysis: Debates and discussion. *Quality & Quantity*, *49*(3), 1135-1143. https://doi:10.1007/s11135-014-0039-2

Chu, H., & Ke, Q. (2017). Research methods: What's in the name? Library & Information Science Research, 39(4). 284-294, https://doi.org/10.1016/j.lisr.2017.11.001

Chung, K., Kamhoua, C. A., Kwiat, K. A., Kalbarczyk, Z. T., & Iyer, R. K. (2016). Game theory with learning for cyber security monitoring, *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, 1-8. https://doi.org/10.1109/HASE.2016.48

Cirnu, C. E., Rotună, C. I., Vevera, A. V., & Boncea, R. (2018). Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. *Studies in Informatics and Control*, *27*(3), 359-368. https://doi.org/10.24846/v27i3y201811

Clandinin, D., Cave, M., & Berendonk, C. (2017). Narrative inquiry: A relational research methodology for medical education. *Medical Education*, *1*, 89. https://doi.org/10.1111/medu.13136

Clark, K. J. (2020). *Crime Analysis Centers: Understanding How CAC's Can Assist with Cyber Security Attacks* [Doctoral dissertation, Utica College]. (2406647154). https://www.proquest.com/dissertations-theses/crime-analysis-centers-understanding-how-cac-s/docview/2406647154/se-2?accountid=14872

Cleveland, S., & Cleveland, M. (2018, May). Toward cybersecurity leadership framework. In *Proceedings of the Thirteenth Midwest Association for Information Systems Conference*. https://www.researchgate.net/

Cobb, M. J. (2018). Plugging the skills gap: the vital role that women should play in cyber-security, *Computer Fraud & Security* 1, 5-8. https://doi.org/10.1016/S1361-

3723(18)30004-6

Cole, E., & Ring, S. (2005). *Insider threat: Protecting the enterprise from sabotage, spying, and theft*. Syngress.

Congress. (2019). H.R.3270 – Active cyber defense certainty act. 116th Congress (2019-2020). The *Active Cyber Defense Act*. https://www.congress.gov

Congress. (2020). H.R. 4246 – Cybersecurity information act. 106th Congress (1999-2000). The Cybersecurity Information Act. https://www.congress.gov

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures, *Computers & Security, 87*, https://doi.org/10.1016/j.cose.2019.101568.

Conteh, N., & Royer, M. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability facto. *International Journal of Computer, 20*(1), 1-12. https://tmuk.pw/zefi-b-z-cygus-ko.pdf

Cook, K. D. (2017). *Effective cyber security strategies for small businesses*. *Walden Dissertations and Doctoral Studies*. 3871. https://scholarworks.waldenu.edu/dissertations/3871

Cook, S. (2022, February 18). Malware statistics and facts for 2022. *Comparitech*. https://www.comparitech.com/antivirus/malware-statistics-facts/

Copes, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research, *Oncology Nursing Forum, 41*(1), 89-91. https://doi.org/10.1188/14.ONF.89-91

Coulson, T., Mason, M., & Nestler, V. (2018). Cyber capability planning and the need for

an expanded cybersecurity workforce. *Communication of the IIMA, 16*(3). https://scholarworks.lib.csusb.edu/ciima/vol16/iss2/2

Crane, B., & Hartwell, C. J. (2018). Developing employees' mental complexity: Transformational leadership as a catalyst in employee development. *Human Resource Development Review*, *17*(3), 234–257. https://doi.org/10.1177/1534484318781439

Creswell, J. W., & Baez, J. C. (2021). *Thirty essential skills for the qualitative researchers*. Sage.

Creswell, J. W., & Guetterman, T. C. (2018). *Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research*. Pearson.

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

Cross, C., Parker, M., & Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *International Review of Victimology, 25*(1), 53-69. https://doi.org/10.1177/0269758017752410

Crumpler, W., & Lewis, J. A. (2019). The Cybersecurity workforce gap. Center for Strategic & International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

Cuthbert, C. A., & Moules, N. (2014). The application of qualitative research findings to oncology nursing practice. *Oncology Nursing Forum, 41*(6), 683-685. https://doi.org/10.1188/14.ONF.683-685

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimension Critical Care Nurse, 36*(4), 253-263. https://doi.org/10.1097/DCC.0000000000000253

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

DeFord, D. F. (2022). Sustainable digital health demand cybersecurity transformation. *Frontiers of Health Services Management 2022 38*(3), 31-38. https://doi:10.1097/HAP.0000000000000137

Deighton, A. (2015). Cybersecurity: the dos, the don'ts, and the legal issues you need to understand. *Financier Worldwide*. https://www.financierworldwide.com

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family medicine and community health*, *7*(2), e000057. https://doi.org/10.1136/fmch-2018-000057

Denscombe, M. (2008). Communities of practice: A research paradigm for the mixed methods approach. *Journal of Mixed Methods*, https://doi.org/10.1177/1558689808316807

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security 2015* (1), 5-8. https://doi.org/10.1016/S1353-4858(15)70007-3.

Department of Homeland Security, United States Government. (2016). National cyber

incident response plan. https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Department of Homeland Security, United States Government. (2020). Cyber Incidents. https://www.dhs.gov/cyber-incidents

Deschamp, C. (2016). Transformational leadership and change: How leaders influence their followers' motivation through organizational justice. *Journal of Healthcare Management, 61*(3), 194-213. https://doi.org/10.1097/00115514-201605000-00007

DiGiacinto, D. (2019). The Importance of the internal review board for approving proposed research. *Journal of Diagnostic Medical Sonography*, *35*(2), 85–86. https://doi.org/10.1177/8756479318817220

DiGrazia, K. (2018). Cyber insurance, data security, and blockchain in the wake of the Equifax breach. *Journal of Business & Technology Law*, *13*(2). https://digitalcommons.law.umaryland.edu/jbtl/vol13/iss2/5/

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., & Iyengar, S. S. (2017). Game theory for cybersecurity and privacy. *ACM Computing Surveys*, 2, 30. https://doi.org/10.1145/3057268

Doody, O., & Doody, C. M. (2015). Conducting a pilot study: Case study of a novice researcher. *British Journal of Nursing, 24*, 1074-1078. https://doi:10.12968/bjon.2015.24.21.1074

Duan, C. (2020). Hacking antitrust: Competition policy and the computer fraud and abuse

act. *Colorado Technology Law Journal, 19*(2), https://ssrn.com/abstract=3707016

Edmonds, E. A. (2017). [Review of the book General System Theory: Foundations, Development, Applications by Ludwig von Bertalanffy]. Leonardo 19(3), 248. https://muse.jhu.edu/article/598665/summary

Emmanuel, E., Abdoler, E., & Stunkel, L. (n.d.). Research ethics: How to treat people Emmanuel who participate in research. National Institute of Health. https://bioethics.nih.gov/education/FNIH_BioethicsBrochure_WEB.PDF

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis, *IEEE Access*, vol. 10, pp. 52319-52335, 2022. https://doi10.1109/ACCESS.2022.3171829

Erickson, A., & Neilson, T. (2018). Cybersecurity – the No. 1 threat facing manufacturers. *Journal of Industrial Management 60*(4), 24 -27.

Erkutlu, H. (2008). The impact of transformational leadership on organizational and leadership effectiveness: The Turkish case. *Journal of Management Development*, *27*(7), 708-726. https://doi.org/10.1108/02621710810883616

Etikan, I., Abubakar, M., & Alkassim, R. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics. 5*(1), 1-4. https://doi:10.11648/j/ajtas.20160501.11

Evans, C., & Lewis, J. (2018). *Analysing semi-structured interviews using thematic analysis: Exploring voluntary civic participation among adults*. SAGE. http://dx.doi.org/10.4135/9781526439284

Fahlevi, M., Zuhri, S., Parashakti, R., & Ekhsan, M. (2019). Leadership styles of food

truck businesses. *Journal of Research in Business, Economics and Management, 13*(2), 2437-2442. https://www.researchgate.net/

Fei, Z., Wang, X., & Wang, Z. (2021). Event-Based Fault Detection for Unmanned Surface Vehicles Subject to Denial-of-Service Attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 1-11. https://doi:10.1109/tsmc.2021.3064884

Feuilherade, P. (2021, October). Cyber security becomes a multi-billion $ market. *The MiddleEast Online*. https://www.themiddleeastmagazine.com/business/business-cyber-security/

FBI. (2020). *Ransomware.* Scams and Safety. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Fernandez, T., Godwin, A., Doyle, J., Verdin, D., Boone, H., Kirn, A., Benson, L., & Potvin, G. (2016). More comprehensive and inclusive approaches to demographic data collection. School of Engineering Education Graduate Student Series. Paper 60. https://docs.lib.purdue.edu/enegs/60

Fofana, F., Bazeley, P., & Regnault, A. (2020). Applying a mixed methods design to test saturation for qualitative data in health outcomes research. *PLoS ONE 15*(6), 1-12. https://doi.org/10.1371/journal.pone.0234898

Franke, U. (2017). The cyber insurance market in Sweden, *Computers & Security 68*, 130-144. https://doi.org/10.1016/j.cose.2017.04.010

Freedman, L. E. (2020). Update ransomware: To pay or not to pay. *The National Law Review, X*(313). https://www.natlawreview.com/article/update-ransomware-to-

pay-or-not-to-pay

Friesen, P., Kerns, L., Redman, B., & Caplan, A. (2017). Rethinking the Belmont report. *The American Journal of Bio Ethics, 17*(7), 15-21. https://doi:10.1080/15265161.2017.1329482

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, *2017*(2), 5–10. https://doi.org/10.1016/S1361-3723(17)30013-1

Gallego-Jimenez, M., Pedraz-Marcos, A., & Graell-Berna, M. (2018). Value of pilot studies in qualitative research: Case of an investigation about non-suicidal self-injury. *Enfermeric Clinica*, *28*(4), 276-278. https://doi.org/10.1016/j.enfcli.2018.02.001

Gañán, C. H., Ciere, M., & Van Eeten, M. (2017). Beyond the pretty penny: the economic impact of cybercrime. *NSPW 2017: 2017 New Security Paradigms Workshop*, 35–45. https://dl.acm.org/doi/10.1145/3171533.3171535

Garcia, A., Zuniga, J., & Lagon, C. (2017). A personal touch: The most important strategy for recruiting Latino research participants. *J Transcultural Nursing, 28*(4), 342-347. https://doi.org/10.1177/1043659616644958

Ge, M., Cho, J. H., Kim, D., Dixit, G., & Chen, I. R. (2021). Proactive defense for internet-of-things: Moving target defense with cberdeception. *ACM Transactions on Internet Technology (TOIT)*, *22*(1), 1-31. https://doi.org/10.1145/3467021

Ghasabeh, M. S., Soosay, C., & Reaiche, C. (2015). The emerging role of transformational leadership. *The Journal of Developing Areas, 49*(6), 459-467.

https://doi:10.1353/jda.2015.0090

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Anal, 1*(6). https://doi.org/10.1186/s41044-016-0006-0

Gliha, D. (2017). Maritime cyber crime – 21st century piracy. *Anali Pravnog Fakulteta Univerziteta u Zenici*, *10*(20), 228–238. https://www.ceeol.com/search/article-detail?id=699426

Goel, S. (2016). Cybercrime: A growing threat to Indian banking sector. 3rd International Conference. *International Journal of Science Technology and Management, 5*(12), 552-559. https://ijstm.com/currentissue.php?id=98

Govender, I., Watson, B. W. W., & Amra, J. (2021). Global virus lockdown and cybercrime rate trends: a routine activity approach. *Journal of Physics: Conference Series, 1828*. https://doi.org//10.1088/1742-6596/1828/1/012107

Goyal, P., Lobiyal, D. K., & Katti, C. P. (2018). Game theory for vertical handoff decisions in heterogeneous wireless networks. A tutorial in Bhattacharyya S., Gandhi, T., Sharma K., Dutta P. (eds) Advance computational and communication paradigms. Lecture Notes in Electrical Engineering, 475. Springer. https://link.springer.com/chapter/10.1007/978-981-10-8240-5_47

Grandpoint Bank. (2016). Grandpoint bank makes first-of-its-kind cyber crime insurance available to protect business accounts from funds transfer fraud and cyber deception. https://www.businesswire.com/news/home/20160621006377/en

Graves, T. (2019). Active cyber defense certainty act. H.R. 3270=116th Congress 2019-

2020. https://www.congress.gov/bill/116th-congress/house-bill/3270/text?q=%7B%22search%22%3A%5B%22active+cyber+defense+act%22%5D%7D&r=4&s=1

Greenleaf, R. K. (1977). *Servant leadership: a journey into the nature of legitimate power and greatness*. Paulist Press.

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

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLOS One*, *15*(5). https://doi.org/10.1371/journal.pone.0232076

Guetterman, T. C., Sakakibara, R. V., Plano Clark, V. L., Luborsky, M., Murray, S. M., Castro, F. G., Creswell, J. W., Deutsch, C., & Gallo, J. J. (2019). Mixed methods grant applications in the health sciences: An analysis of reviewer comments. *Journal PLOS ONE*, https://doi.org/10.1371/journal.pone.0225308

Guillemin, M., Barnard, E., Allen, A., Stewart, P., Walker, H., Rosenthal, D., & Gilliam, L. (2018). Do research participants trust researchers or their institution? *Journal of Empirical Research on Human Research Ethics, 13*(3), 285-294. https://doi.org/10.1177/1556264618763253

Guillemin, M., Gillam, L., Barnard, E., Stewart, P., Walker, H., & Rosenthal, D. (2016). Doing trust: How researcher conceptualize and enact trust in their research practice. *Journal of Empirical Research on Human Research Ethics, 11*, 370-381.

https://doi.org/10.1177/1556264616668975

Guo, H., Cheng, H. K., & Kelley, K. (2016). Impact of network structure on malware propagation: A growth curve perspective. *The Journal of Management Information Systems*, *33*(1), 296-325. https://doi.org/10.1080/07421222.2016.1172440

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. Academy of Business, Engineering and Science, Halmstad University, Halmstad, Sweden. https://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714. https://doi:10.1080/074221222.2018.1451962

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction, 31*(3), 498-501. https://doi:10.1093/humrep/dev334

Hammond, D. (2010). The science of synthesis: Exploring the social implications of general system theory. University Press of Colorado.

Han, S.-H., Oh, E. G., & Kang, S. (2020). The link between transformational leadership and work-related performance: moderated-mediating roles of meaningfulness and job characteristics, *Leadership & Organization Development Journal*, *41*(4), 519-533. https://doi.org/10.1108/LODJ-04-2019-0181

Hancock, M. E., Amankwaa, L., Revell, M. A., & Mueller, D. (2016). *The Qualitative Report 21*(11), 2124-2130. https://search.proquest.com/openview/df220566b53a6853f15ac561bb7af91b/1?pq-origsite=gscholar&cbl=55152

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security, 95*. https://doi.org/10.1016/j.cose.2020.101827

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

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human. *Computer & Security 76.* 101-127. https://doi.org/10.1016/j.cose.2018.02.020

Heath, B. (2018). Before the breach: The role of cyber insurance in incentivizing data security. *The George Washington Law Review, 86*(4). https://www.gwlr.org/wp-content/uploads/2018/09/86-Geo.-Wash.-L.-Rev.-1115.pdf

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*, 30–38. https://doi.org/10.1016/j.techsoc.2015.11.007

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code Saturation Versus Meaning Saturation: How Many Interviews Are Enough? *Qualitative Health Research, 27*(4), 591–608. https://doi.org/10.1177/1049732316665344

Ho, S. M., & Gross, M. (2021). Consciousness of cyber defense: A collective activity

system for developing organizational cyber awareness. *Computers & Security 108* https://doi.org/10.1016/j.cose.2021.102357

Hoch, J. E., Bommer, W. H., Dulebohn, J. H., & Wu, D. (2018). Do ethical, authentic, and servant leadership explain variance above and beyond transformational leadership? A meta-analysis. *Journal of Management*, *44*(2), 501–529. https://doi.org/10.1177/0149206316665461

Holdsworth, J., & Apeh, E. (2017). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector, *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*, Lisbon, 2017, 111-117. https://doi.org/10.1109/REW.2017.47

Holloway, I., & Galvin, K. (2017). *Qualitative research in nursing and healthcare* (4th ed), Wiley Blackwell.

Hostrup M. & Anderson, B. L. (2020). Leading to make a difference for whom? How vision content moderates the relationship between transformational leadership and public service motivation. *International Public Management Journal*, https://doi.org/10.1080/10967494.2020.1795015

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: an example from practice. *Nurse Researcher*, *22*(5), 8-12. https://journals.rcni.com/nurse-researcher/qualitative-case-study-data-analysis-an-example-from-practice-nr.22.5.8.e1307

IBM *Security*. (2022). Cost of a data breach report 2021. https://ibm.com/security/data-breach

Idahosa, M. D. (2020). Strategies for implementing successful IT security systems in small businesses. *Walden Dissertations and Doctoral Studies*. 8546. https://scholarworks.waldenu.edu/dissertations/8546

Iovan, S., & Iovan, A. (2016). From cyber threats to cybercrime. *Journal of Information Systems & Operations Management, 10*(5), 425- 434. http://www.rebe.rau.ro/RePEc/rau/jisomg/WI16/JISOM-WI16-A15.pdf

Iwu, C. G., Kapondoro, L., Twum-Darko, M., & Lose, T. (2016). Strategic human resource metrics: A perspective of the general systems theory. *Acta Universitatis Danubius Oeconomica 12*(2): 5–24. https://journals.univ-danubius.ro/index.php/oeconomica/article/view/3191/3218

Jaafar, G., Abdullah, S., & Ismail, S. (2019). Review of recent detection methods for http DDoS attack. *Journal of Computer Networks and Communications*, 2019. https://doi.org/10.1155/2019/1283472

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

Javed Butt, U., Abbod, M., Lors, A., Jahankhani, H., Jamal, A., & Kumar, A. (2019). Ransomware Threat and its Impact on SCADA. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), Global Security, Safety and Sustainability (ICGS3), 2019 IEEE 12th International Conference On*, 205–212. https://ieeexplore.ieee.org/document/8688327

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*

2020 84(1). https://doi.org/10.5688/ajpe7120

Jones, D. (2022, April 27). Ransomware attacks, payouts soared worldwide in 2021: report. Cybersecurity Dive. https://www.cybersecuritydive.com/news/ransomware-attacks-payouts-2021/622784/

Joslin, R., & Muller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management, 34*(6), 1043-1056. https://doi.org/10.1016/j.ijproman.2016.05.005

Juniper Research. (2019, August 27). Business losses to cybercrime data breaches to exceed $5 trillion by 2024 [Press release]. https://www.businesswire.com/news/home/20190826005013/en/Business-Losses-Cybercrime-Data-Breaches-Exceed-5

Kadam, R. A. (2017). Informed consent process: A step further towards making it meaningful! *Perspectives in clinical research*, *8*(3), 107–112. https://doaj.org/article/dcdc38eab9c14763a1c94cfbcb6937fa

Kans, M. (2018). A congressional cybersecurity to-do list. *Just Security*. https://www.justsecurity.org/61480/congressional-cybersecurity-to-do-list/

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: The power of reflexivity. *International Journal of Interdisciplinary Educational Studies*, *13*(1), 19–31. https://doi.org/10.18848/2327-011X/CGP/v13i01/19-31

Katrakazas, P., Pastiadis, K., Bibas, A., & Koutsoures, D. (2020). A general systems theory approach in public hearing health: Lessons learned from a systematic

review of general systems theory in healthcare. *IEEE Access*, *8*, 53018-53033. https://ieeexplore.ieee.org/document/9037270

Keets, J., & Abaldo, A. (2017). Servant leadership: Learning from servant leaders of the past and their impact to the future. *International Journal of Management Sciences and Business Research, 6*(1). https://ssrn.com/abstract=2912730

Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education, 2*. https://commons.erau.edu/db-security-studies

Khan, N. A., Khan, A. N., Soomro, M. A., & Khan, S. K. (2020). Transformational leadership and civic virtue behavior: Valuing act of thriving and emotional exhaustion in the hotel industry. *Asia Pacific Management Review*, *25*(4), 216–225. https://doi.org/10.1016/j.apmrv.2020.05.001

Khan, S., Gani, A., Wahab, A. W. A., & Singh, P. K. (2018). Feature selection of denial-of-service attacks using entropy and granular computing. *ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING*, *43*(2), 499–508. https://link.springer.com/article/10.1007/s13369-017-2634-8

Khimani, H., & Parekh, C. (2017). IoT security and hardware implementation using DTMF 8870. *International Journal of Advanced Research in Computer Science*, *8*(5), 2403–2406. https://www.ijarcs.info/index.php/Ijarcs/article/view/3461

Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective, *IEEE Access*, 8, 78847-78867. https://ieeexplore.ieee.org/document/9078082

Klitzman, R. (2019). *The ethics police? The struggle to make human research safe*. Oxford Press.

Kok, S. H., Abdullah A., Jhanjhi N., & Supramaniam M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. *Computers*, *8*(4). https://doi.org/10.3390/computers8040079

Kolouch, J. (2018). Evolution of phishing and business email compromise campaignes in the Czech Republic. *Academic and Applied Research in Military and Public Management Science*, *17*(3), 83-100. https://folyoirat.ludovika.hu/index.php/aarms/article/view/1068

Krawczyk, P., Topolewski, M., & Pallot, M. (2017). Towards a reliable and valid mixed methods instrument in user experience studies. Paper presented at *2017 International Conference on Engineering, Technology, and Innovation (ICE/ITMC)*, Funchal, Portugal. https://www.researchgate.net/

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology. *Journal of Parapsychology*, *79*(2), 219-233. https://search.proquest.com/openview/27127bb8d0ea9fad6d8f02ea3c382ad3/1?pq-origsite=gscholar&cbl=42308

Kuckartz, U., & Radiker, S. (2019). *Documenting and archiving the research process: Analyzing qualitative data with MAXQDA.* Springer. https://doi.org/10.1007/978-3-030-15671-8

Kumar, S., & Carley, K. M. (2016). Approaches to understanding the motivations behind cyber-attacks," *2016 IEEE Conference on Intelligence and Security Informatics*

(ISI), Tucson, AZ, 2016, 307-309. https://doi.org/10.1109/ISI.2016.7745496

Kumari, N., & Majumder, S. (2021). The impact of teamwork and other factors for team effectiveness on work performance of employees. *Innovative Management Practices—An Interdisciplinary Approach with Special Reference to the New Normal; Syedain, G., Kumar, A., Eds*, 227-232.

Kurpjuhn, T. (2019). The guide to ransomware: How businesses can manage the evolving threat. *Computer Fraud & Security 2019*(11). https://doi.org/10.1016/S1361-3723(19)30117-4

Kuusisto, T., & Kuusisto, R. (2016). Leadership for cyber-security in public-private relations. https://www.researchgate.net

Lancaster, K. (2017). Confidentiality, anonymity, and power relations in elite interviewing conducting qualitative policy research in a politicized domain. *International Journal of Social Research Methodology, 1*, 1-11. https://doi:10.1080/13645579.2015.1123555

Lantos, J. D. (2020). The Belmont report and innovative clinical research. Perspectives in Biology and Medicine 63(2), 389-400. https://doi:10.1353/pbm.2020.0026

Le, D. C., & Zincir-Heywood, A. N. (2018). Evaluating insider threat detection workflow Using supervised and unsupervised learning. *2018 IEEE Security and Privacy Workshops (SPW)*, 270-275. https://doi:10.1109/SPW.2018.00043

Ledesma, J. (2014). Conceptual Frameworks and Research Models on Resilience in Leadership. *SAGE Open*. https://doi.org/10.1177/2158244014545464

Lee, V. (2018). Beyond seeking informed consent: Upholding ethical values within the

research proposal. *Canadian Oncology Nursing Journal = Revue Canadienne de Nursing Oncologique*, *28*(3), 222-224. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6516914/

Legard, R., Keegan, J., & Ward, K. (2003). *In-depth interviews. Qualitative research practice: A guide for social science students and researchers*. Sage.

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139-148. https://doi.org/10.1080/19393555.2020.1813851

Lekha, K. C., & Prakasam, S. (2018). Implementation of data mining techniques for cybercrime detection. *International Journal of Engineering, Science and Mathematics 7*(4). https://www.ijesm.co.in/abstract.php?article_id=5628&title=IMPLEMENTATION%20OF%20DATA%20MINING%20TECHNIQUES%20FOR%20CYBER%20CRIME%20DETECTION

Lekota, F., & Coetzee, M. (2019). Cybersecurity incident response for the sub-saharan African aviation industry. In *International Conference on Cyber Warfare and Security* (pp. 536-XII). Academic Conferences International Limited. https://www.proquest.com/conference-papers-proceedings/cybersecurity-incident-response-sub-saharan/docview/2198531213/se-2?accountid=14872

Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using lexi-mancer for qualitative data analysis triangulation. *Qualitative Report*, *25*(3), 604–614. https://nsuworks.nova.edu/tqr/vol25/iss3/

Lertora, I. M., & Sullivan, J. (2019). The lived experiences of Chinese international students preparing for the university-to-work transition: A phenomenological qualitative study. *The Qualitative Report*, *24*(8), 1877-1896. https://nsuworks.nova.edu/tqr/vol24/iss8/

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to Do Qualitative Data Analysis: A Starting Point. *Human Resource Development Review*, *19*(1), 94–106. https://doi.org/10.1177/1534484320903890

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. Journal *of Family Medicine and Primary Care, 4*(3). https://www.ncbi.nlm.nih.gov/pmc/articles/Pmc4535087/

Li, Y., Deng, S., & Zhang, Y. (2019). Research on the motivation to contribution and influencing factors of university students: A semi-structured interview based on qualitative research. IOP Conf. Series: Materials Science and Engineering 563 (2019) 052095 IOP Publishing. https://iopscience.iop.org/article/10.1088/1757-899X/563/5/052095/pdf

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Sage.

Lindros, K., & Tittel, E. (2016). What is cyber insurance and why you need it. CSO United States. https://www.csoonline.com/article/3065474/what-is-cyber-insurance-and-why-you-need-it.html

Liu, L., De Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. *IEEE Communications Surveys & Tutorials*, *20*(2), 1397-1417. https://ieeexplore.ieee.org/abstract/document/8278157

Lopreato, J. (1970). General system theory: Foundations, development, applications (book). *American Sociological Review*, 35(3), 543-545. https://doi.org/10.2307/2093003

Lyon, V. (2020). Exploring strategies for recruiting and retaining diverse cybersecurity professional. Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/dissertations/8307

Machi, L. A., & McEvoy, B. T. (2016). *The literature review Six steps to success*. Sage.

Macias, C. J. G., & Contreras, T. J. C. (2019). The life story: A social qualitative research Method and its application in tourism management studies. *Revista Iberoamericana de Turismo- RITUR, Penedo, 9*, 59-77. https://www.seer.ufal.br/index.php/ritur/article/download/8686/6544

Maguire, M., & Delahunt, B. (2017). Doing thematic analysis: A practical step-by-step guide for Learning and teaching scholars. *All Ireland Journal of Higher Education 9* (3). https://ojs.aishe.org/index.php/aishe-j/article/view/335/553

Majid, M. A., Othman, M., Mohamad, S. F., Lim, S. A., & Yusof, A. (2017). Piloting for interviews in qualitative research: Operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences 7*(4), 2222-6990. https://www.semanticscholar.org/paper/Piloting-for-Interviews-in-Qualitative-Research%3A-Majid-Othman/78bf0ddda8859fdc0839aba619d42715ce43080c

Mania-Singer, J. (2017). A systems theory approach to the district central office's role in school level improvement. *Administrative Issues Journal 4*(1) 70-83.

https://eric.ed.gov/?id=EJ1151585

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

Marion, T. J., Eddleston, K. A., Friar, J. H., & Deeds, D. (2015). The evolution of interorganizational relationships in emerging ventures: An ethnographic study within the new product development process. *Journal of Business Venturing, 30* (1), 167-184. https://www.effectuation.org/wp-content/uploads/2017/06/The-evolution-of-interorganizational-relationships-in-emerging-ventures-An-ethnographic-study-within-the-new-product-development-process-1.pdf

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. https://cordis.europa.eu/project/id/734815

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

Martin, H. C., Rogers, C., Samuel, A. J., & Rowling, M. (2017). Serving from the top: police leadership for the twenty-first century. *International Journal of Emergency Services*, *6*(3), 209–219. https://researchoutput.csu.edu.au/en/publications/serving-from-the-top-police-leadership-for-the-21st-century

Maxwell, J. A. (2021). Why qualitative methods are necessary for generalization. *Qualitative Psychology*, *8*(1), 111–118. https://doi.org/10.1037/qup0000173

Mazzarolo, G., & Jurcut, A. D. (2020). Insider threats in cyber security: The enemy within the gates. *European Cybersecurity Journal*,

https://arxiv.org/abs/1911.09575

McCreless, P. (2022, March 22). South carolina residents lost $42 million to cyber crime in 2021. Government Technology. https://www.govtech.com/security/south-carolina-residents-lost-42m-to-cyber-crime-in-2021

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

Meland, P. H., & Seehusen, F. (2018). When to treat security risks with cyber insurance. *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Glasgow, 1-8. https://ieeexplore.ieee.org/abstract/document/8551456

Merriam, S. B. (2014). *Qualitative research: A guide to design and implementation* (3rd ed.). Wiley.

Mishra, A. K., Tripathy, A. K., & Swain, S. (2018). Analysis and prevention of phishing attacks in cyber space. 2018 First International Conference on Securre Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2018, 430-434. https://ieeexplore.ieee.org/abstract/document/8703343

Mishra, S., Alowaidi, M. A., & Sharma, S. K. (2021). Impact of security standards and policies on the credibility of e-government. *J Ambient Intell Human Comput*. https://doi.org/10.1007/s12652-020-02767-5

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransonware attack 2017. International Journal of Advanced Research in Computer Science 8(5).

https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Money, V. (2017). Effectiveness of transformation leadership styles in secondary schools in Nigeria. *Journal of Education and Practices, 8* (9), 135-140. https://eric.ed.gov/?id=EJ1138836

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry *Current Psychiatry Reports 23*(18). https://doi.org/10.1007/s11920-021-01228-w

Montgomery, E. G., & Oladapo, V. (2014). Talent management vulnerabilities in global healthcare value chains: A general systems theory perspective. *Journal of Business Studies Quarterly, 5*(4). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.652.8943&rep=rep1&type=pdf

Moore, R., (2022). Incident response team: What are the roles and responsibilities. *AT&T Cybersecurity*. https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team

Morse, J. M. (1995). Significance of saturation. *Qualitative Health Research, 5*(2) 147-149. Sage. https://journals.sagepub.com/doi/pdf/10.1177/104973239500500201

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

Mutlak, F. (2017). Building a cyber security strategy: The three lines of defence model allows leaders to address the diverse risks of the digital world. *MEED Business*

Review, *2*(12), 34–35. https://www.meed.com/latest/meed-business-review

Mwiraria, D. R., Ngetich, K., & Mwaeke, P. (2022). Factors associated with cybercrime awareness among university students in Egerton university, Njoro campus, Kakuru county, Kenya. *European Journal of Humanities and Social Sciences 2*(3), 63-68. http://dx.doi.org/10.24018/ejsocial.2022.2.3.256

Naeem, M., & Ozuem, W. (2021). The role of social media in internet banking transition during COVID-19 pandemic: Using multiple methods and sources in qualitative research. *Journal of Retailing and Consumer Services*, 30. https://doi.org/10.1016/j.jretconser.2021.102483

Nasution, M., Rossanty, Y., Siahaan, H., & Arysam, S. (2018). The phenomenon of cyber-crime and fraud victimization in online shop. *International Journal of Civil Engineering and Technology*, *9*(6), 1583-1592. https://www.researchgate.net/

National Institute of Standards and Technology (NIST). (2019). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). NICE cybersecurity workforce framework: National initiative for cybersecurity education. Special Publication (NIST SP) - 800-181. https://doi.org/10.6028/NIST.SP.800-181

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence-Based Nursing*, *22*(3), 67–68. https://ebn.bmj.com/content/ebnurs/22/3/67.full.pdf

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research.

Evidence Based Nurse, 18(2). https://dx.doi.org/10.1136/eb-2015-102054

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

Nyide, C. J. (2020). Effective leadership styles for cooperative banks in an emerging economy. *Journal of Legal, Ethical and Regulatory Issues 23*(3), 1-14. https://hdl.handle.net/10321/3510

Nyström, M. E., Karltun, J., Keller, C., & Gare, B. A. (2018). Collaborative and partnership research for improvement of health and social services: researcher's experiences from 20 projects. *Health Res Policy Sys 16***,** 46. https://doi.org/10.1186/s12961-018-0322-0

Oh, J., Kim, T. H., & Lee, K. H. (2019). Advanced insider threat detection model to apply periodic work atmosphere. *KSII Transactions on Internet & Information Systems*, *13*(3), 1722–1737. https://www.sciencegate.app/document/10.3837/tiis.2019.03.035

O'Kane, P., Smith, A., & Lerman, M. P. (2021). Building Transparency and Trustworthiness in Inductive Research Through Computer-Aided Qualitative Data Analysis Software. *Organizational Research Methods*, *24*(1), 104–139. https://doi.org/10.1177/1094428119865016

Paganini, P. (2020). How botnets are evolving from Iot botnets to hivnets. Cybernews. https://cybernews.com/security/how-botnets-are-evolving-from-iot-botnets-to-hivenets/

Parker, C. F., Karlsson, C., & Hjerpe, M. (2017). Assessing the European union global climate change leadership: from Copenhagen to the Paris agreement. *Journal of European Integration, 39*(2) 239-252 https://doi.org/10.1080/07036337.2016.1275608

Pascanu, R., Stokes, J. W., Sanossian, H., Marinescu, M., & Thomas, A. (2015). Malware classification with recurrent networks, *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brisbane, QLD, 1916-1920. https://ieeexplore.ieee.org/document/7178304

Patyal, M., Sampalli, S., Ye, Q., & Rahman, M. (2017). Multi-layered defense architecture against ransomware. *International Journal of Business & Cybersecurity, (1)*2, 52-64. https://www.researchgate.net

Paulus, T., Woods, M., Atkins, D. P., & Macklin, R. (2017). The discourse of QDAS: reporting practices of ATLAS.ti and NVivo users with implications for best practices, International *Journal of Social Research Methodology, 20*(1), 35-47. https://doi.org/10.1080/13645579.2015.1102454

Perez, M., & Suek, J. (2019). Spotlight: Bank's face growing cybercrime threat. Southwest Economy, Federal Reserve Bank of Dallas, issue Fourth Quarter. https://ideas.repec.org/a/fip/feddse/87589.html

Peter, A. S. (2017). Cyber resilience preparedness of Africa's top 12 emerging economies. *International Journal of Critical Infrastructure Protection, 17*. 49-59. https://doi.org/10.1016/j.ijcip.2017.03.002

Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-

insurance (January 17, 2018). Macquarie University Faculty of Business & Economics Research Paper. https://ssrn.com/abstract=3200166

Peticca-Harris, A., deGama, N., & Elias, S. R. T. A. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods, 19*(3), 376-401. https://doi.org/10.1177/1094428116629218

Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S., & Aiken, M.P. (2022). Conceptualizing cybercrime: Definitions, typologies, and taxonomies. *Forensic Sci. 2*, 379-398. https://doi.org/10.3390/forensicsci2020028

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224–232. https://pubmed.ncbi.nlm.nih.gov/30857581/

Phipps, W. D. (2019). Toward an integrative approach: Refiguring essential developments in family therapy. *Journal of Family Psychotherapy 30*(2), 116-140. https://doi.org/10.1080/08975353.2019.1601447

Ponemon, L. (2018). Calculating the cost of a data breach in 2018, the age of AI and the IOT. *Security Intelligence*. https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Prabowo, H. Y. (2020). Reinvigorating the human instrument: An exploratory study on the potential use of CAQDAS in qualitative evaluation of corruption prevention in Indonesia. *Journal of Financial Crime, 27*(2), 505-530. https://doi.org/10.1108/JFC-01-2019-0004

Prayudi, Y., & Yusirwan, S. (2015). The recognize of malware characteristics through

static and dynamic analysis approach as an effort to prevent cybercrime activities. *Journal of Theoretical and Applied Information Technology, 77*(3), 438-445. https://www.researchgate.net/

Purwanto, A., Bernarto, I., Asbari, M., Wijayanti, L. M., & Hyun, C. C. (2020). Effect of transformational and transactional leadership style on public health centre performance. *Journal of Research in Business, Economics, and Education 2*(1). https://e-journal.stie-kusumanegara.ac.id

Queiros, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*, *3*(9). https://oapub.org/edu/index.php/ejes/issue/view/76

Radanliev, P., De Roure, D., Cannady, S., Mantila Montaluq, R., Nicolescu, R., & Huth, M. (2018). Living in the internet of things: Cybersecurity of the IoT - 2018. IET Conference Proceedings. *The Institution of Engineering and Technology* London 1-9. https://hdl.handle.net/10419/193692

Raghavan, R. (2018). Cyber insurance – A risk mitigation tool for cyber risk in India. *Bimaquest*, *18*(1). https://www.bimaquest.niapune.org.in/index.php/bimaquest/article/view/17

Rahman, M. S. (2017). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “testing and assessment” research: A literature review. *Journal of Education and Learning*, *6*(1), 102–112. http://dx.doi.org/10.5539/jel.v6n1p102

Rana, S. (2018). Managing businesses relevance beyond technology. *FIIB Business*

Review, *7*(4), 229–231. https://doi.org/10.1177/2319714518818231

Reed, E., & Scott, K. (2018). You may be able to outsource privacy and cybersecurity functions, but you can't outsource the risk of liability. *Comm. Law.*, *33*, 4. https://heinonline.org/HOL/LandingPage?handle=hein.journals/comlaw33&div=31&id=&page=

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*. https://doi.org/10.1177/21582440211000049

Reis, L. P., Costa, A. P., & de Souza, F. N. (2016). A survey on computer assisted qualitative data analysis software, *2016 11th Iberian Conference on Information Systems and Technologies (CISTI)*, Las Palmas, 1-6. https://doi: 10.1109/CISTI.2016.7521502

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*(5), 824–831. https://doi.org/10.1177/1049732317753586

Resnik, D. B. (2018). The Ethics of Research with Human Subjects: Protecting People, Advancing Science, Promoting Trust, Springer. https://doi.org/10.1007/978-3-319-68756-8

Rid, T., & Buchanan, B. (2015). Attributing cyberattacks. *Journal of Strategic Studies* *38*(1-2), 4-37. https://doi:10.1080101402390.2014.977382

Ridder, H. G. (2017). The theory contribution of case study research designs. *Business Research* 10, 281-301. https://doi.org/10.1007/s40685-017-0045-z

Roberts, K., Dowell, A., & Nie, J. (2019). Attempting rigour and replicability in thematic analysis of qualitative research data; a case study of codebook development. *BMC Medical Research Methodology 19*. https://doi.org/10.1186/s12874-019-0707-y

Roberts, R. E. (2020). Qualitative Interview Questions: Guidance for Novice Researchers. *The Qualitative Report, 25*(9), 3185-3203. https://www.proquest.com/scholarly-journals/qualitative-interview-questions-guidance-novice/docview/2445581779/se-2

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security, 49,* 70-94. https://doi: 10.1016/j.cose.2014.11.007

Rodbert, M. (2020). Why organizational readiness is vital in the fight against insider threat. *Network Security, 2020*(8), 7-9. https://doi.org/10.1016/S1353-4858(20)30092-1

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

Rousseau, D. (2015). General systems theory: It's present and potential. *Systems Research and Behavior Science 32*(5), 522-533. https://doi.org/10.1002/sres.2354

Rubio, J. E., Alearaz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security Journal 87*(1). https://doi.org/10.1016/j.cose.2019.06.015

Rudd, E. M., Rozsa, A., Günther, M., & Boult, T. E. (2017). A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions, *IEEE Communications Surveys & Tutorials, 19*(2), 1145-1172. Secondquarter

2017. https://doi.org/10.1109/COMST.2016.2636078

Russell, G. (2017). Resisting the persistent threat of cyber-attacks. *Computer Fraud & Security* (12). 7-11. https://doi.org/10.1016/S1361-3723(17)30107-0

Salo, F., Injadat, M., Nassif, A. B., Sham, A., & Essex, A. (2018). "Data Mining Techniques in Intrusion Detection Systems: A Systematic Literature Review," in *IEEE Access*, 6, 56046-56058. https://doi:10.1109/ACCESS.2018.2872784

Santanna, J. J., van Ryswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L., & Pras, A. (2015). Booters — An analysis of DDoS-as-a-service attacks, *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, Ottawa, ON, 2015, 243-251. https://doi.org/10.1109/INM.2015.7140298

Saragih, Y. M., & Siahaan, A. P. (2016). Cyber-crime prevention strategy in Indonesia. *SSRG International Journal of Humanities and Social Science, 3*(6). https://pdfs.semanticscholar.org/0630/448698a02702dc084dfd721aad48372126a5.pdf

Sarma, S. (2015). Data collection in organizational research: Experiences from field. *International Journal of Rural Management, 11*(1), 75-81. https://doi.org/10.1177/0973005215569384

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. *Qual Quant 52*. 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Sawatsky, A. P., Ratelle, J. T., & Beckman, T. J. (2019). Qualitative Research Methods in Medical Education. *Anesthesiology, 131(1)*, 14–22. https://doi.org/10.1097/ALN.0000000000002728

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525-2556. https//doi.org/10.1109/COMST.2021.3117338

Schultz, E. E. (2015). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526-531. https://doi.org/10.1016/S0167-4048(02)01009-X

Schulze, H. (2018). Ninety percent of organizations are vulnerable to insider threats according to new cybersecurity report. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/ninety-percent-organizations-vulnerable-insider-threats-according-new-cybersecurity-report/

Serra, M., Psarra, S., & O'Brien, J. (2018). Social and physical characterization of urban contexts: Techniques and methods for quantification, classification, and purposive sampling. *Urban Planning*, *3*(1). https://dx.doi.org/10.17645/up.v3i1.1269

Setia, M. (2016). Methodology series module 5: Sampling strategies. *Indian Journal of Dermatology, 61*(5), 505-509. https://doi 10.410/0019-5154.190118

Seto, S., & Sarros, J. C. (2016). Servant leadership influence on trust and quality relationship in organizational settings. *International Leadership Journal*, *8*(3), 23–33. https://www.researchgate.net

Sezgin, D., O'Donovan, M., Cornally, N., Liew, A., & O'Caoimh, R. (2019). Defining frailty for healthcare practice and research: A qualitative systematic review with thematic analysis, *International Journal of Nursing Studies, 92*, 16-26. https://doi.org/10.1016/j.ijnurstu.2018.12.014

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: Promising organizational practices. *Information Technology & People 32*(5), 1125-1129. https://doi.org/10.1108/ITP-10-2019-564

Sharma, G. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research, 3*(7), 749-752. https://www.allresearchjournal.com

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*, 63-75. https://doi.org/10.3233/EFI-2004-22201

Simmonds, M. (2017). How businesses can navigate the growing tide of ransomware attacks. *Journal of Computer Fraud & Security, 2017* (3), 9-12. https://doi.org/10.1016/S1361-3723(17)30023-4

Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *The Qualitative Report, 21*(2), 376-392. https://nsuworks.nova.edu/tqr/vol21/iss2/12

Skeoch, H. (2022). Expanding the Gordon-Leob model to cyber-insurance. *Computers & Security 112*(6), https://doi.org/10.1016/j.cose.2021.102533

Smedinghoff, T. J. (2008). The legal challenges of implementing electronic transactions. *Uniform Commercial Code Law Journal, 41*(3),

https://ssrn.com/abstract=1275108

Smedinghoff, T. J. (2015). An overview of data security legal requirements for all business sectors (October 8, 2015). *SSRN*. https://dx.doi.org/10.2139/ssrn.2671323

Smith, J., & Firth, J. (2011). Qualitative data analysis: application of the framework approach. *Nurse Researcher, 18* (2), 52-62. https://pubmed.ncbi.nlm.nih.gov/21319484

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

Sorensen, A. (2018). Warrior women: A phenomenological study of female veterans transitioning into and through college. US Department of Education. https://files.eric.ed.gov/fulltext/ED588089.pdf

Spiers, J., Morse, J. M., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/commentary on a past article: "Verification strategies for establishing reliability and validity in qualitative research": *International Journal of Qualitative Methods*. https://doi.org/10.1177/1609406918788237

Stephen, J. (2016). Cyber-liability insurance is expensive, but can you afford to go uncovered? *Wisconsin Law Journal*. https://search.proquest.com/docview/1815253675?pq-origsite=gscholar&fromopenview=true

Stone, G. A., Russell, R. F., & Patterson, K. (2004). Transformational versus servant

leadership: a difference in leader focus. *Leadership & Organization Development Journal*, *25*(4), 349-361. https://doi.org/10.1108/01437730410538671

Straub, J. (2020). Software engineering: The first line of defense for cybersecurity. 2020 *IEEE 11th International Conference on Software Engineering and Service Science (ICSESS),* 1-5. https://doi.org/10.1109/ICSESS49938.2020.9237715

Suresh, P. V., & Madhavu, M. L. (2022). Insider threat detection in organization using machine learning. *Journal of Applied Information Science 10*(1), 17-28. http://www.publishingindia.com/jais

Taeuscher, K., & Laudien, S. M. (2018). Understanding platform business models: A mixed methods study of marketplaces. *European Management Journal, 36*(3), 319-329. https://doi.org/10.1016/j.emj.2017.06.005

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers' for business. *Law & Social Inquiry 43*(2), 417-440. https://cpri.uci.edu/wp-content/uploads/Talesh-2018-Law_Social_Inquiry-Cyber.pdf

Tarafdar, P., & Bose, I. (2019). Systems theoretic process analysis of information security: the case of aadhaar. *Journal of Organizational Computing and Electronic Commerce, 2*(3), 209-222. https://doi.org/10.1080/10919392.2019.1598608

Teymourlouei, H., & Harris, V., (2019). Effective methods to monitor IT infrastructure security for small business, *2019 International Conference on Computational Science and Computational Intelligence (CSCI),* 2019, 7-13.

https://doi:10.1109/CSCI49370.2019.00009

The White House, United States Government. (2013). Executive order: Executive order -- improving critical infrastructure cybersecurity. Washington, DC. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Tian, H., Iqbal, S., Akhtar, S., Ali Qalati, A., Anwar, F., & Khan M. (2020). The impact of transformational leadership on employee retention: Mediation and moderation through organizational citizenship behavior and communication. *Frontiers in Psychology*, *11*, https://doi.org/10.3389/fpsyg.2020.00314

Tongco, M. D. (2007). Purposive sampling as a tool for informant selection. *Journal of Ehtnobotany, 5,* 147-158. https://www.ethnobotanyjournal.org/index.php/era/article/download/126/111

Toth, P. (2017). *NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*. US Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.HB.162

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

Townsend, K. (2018). NIST small business cybersecurity act becomes law. *Security Week.* https://www.securityweek.com/nist-small-business-cybersecurity-act-becomes-law

Trautman, L. J., & Ormerod, P. C. (2017). Corporate directors' and officers' cybersecurity standard of care: The yahoo data breach. *American University Law Review 66*(5), Article 3. https://digitalcommons.wcl.american.edu/aulr/vol66/iss5/3

Trochin, W. M. K. (2006). Nonprobability sampling. Research methods knowledge base Conjoint.ly. https://www.socialresearchmethods.net/kb/sampnon.php

Vincent, A. (2019). Don't feed the phish, how to avoid phishing attacks. *Network Security 2019*(2). 11-14. https://doi.org/10.1016/S1353-4858(19)30022-4

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal, (4)*2, 32-42. https://search.informit.org/doi/abs/10.3316/informit.093144667545339

Von Bertalanffy, L. (1968). General systems theory: Foundations, development, application (Rev. ed.). George Braziller. http://repository.vnu.edu.vn/handle/VNU_123/90608

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal*, *15*(4), 407–426. https://www.jstor.org/stable/255139

Wei, F., Qin, H., Ye, S., & Zhao, H. (2018). Empirical study of deep learning for text classification in legal document review, *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, 3317-3320. https://ieeexplore.ieee.org/document/8622157

Weller, S. C., Vickers, B., Bernard, H. R., Blackburn, A. M., Borgatti, S., Gravlee, C. C., & Johnson, J. C. (2018). Open-ended interview questions and saturation. *PLoS ONE*, *13*(6). https://doi.org//10.1371/journal.pone.0198606

Wertheim, S. (2019). What to do in the event of a cyberattack. *The CPA Journal*. https://www.cpajournal.com/2019/11/22/what-to-do-in-the-event-of-a-cyberattack/

Whitney, K., Bradley, J. M., Baugh, D. E., & Chesterman, C. W. (2015). System theory as a foundation for governance of complex systems. *International Journal of System of Systems Engineering*, *6*(1-2). https://doi:10.1504/IJSSE.2015.068805

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people? *Business Information Review*, *33*(2), 94-99. https://doi.org/10.1177/0266382116650299

Wilk, A. (2016). Cyber security education and Law, *2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE)*, Beer-Sheva, 94-103. https://doi.org/10.1109/SWSTE.2016.21

Wolgemuth, J. R., Hicks, T., & Agosto, V. (2017). Unpacking Assumptions in Research Synthesis: A Critical Construct Synthesis Approach. *Educational Researcher*, *46*(3), 131–139. https://doi.org/10.3102/0013189X17703946

Wright, J. (2022). Cyber resilient? *The Agent*, *55*(2), 16-17. https://search.informit.org/doi/10.3316/informit.391752553139973

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

Yang, C., Liang, P., & Avgeriou, P. (2018). Assumptions and their management in software development: A systematic mapping study. *Information and Software*

Technology Journal, *94*, 82-110. https://doi.org/10.1016/j.infsof.2017.10.003

Yasir, M., & Mohamad, N. (2016). Ethics and morality: Comparing ethical leadership with servant, authentic and transformational leadership styles. *International Review of Management and Marketing*, *4*, 310. https://www.researchgate.net/

Yazan, B. (2015). Three approaches to case study methods in education: Yin, merriam, and stake. *The Qualitative Report*, *20*(2), 134-152. https://nsuworks.nova.edu/tqr/vol20/iss2/12/

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial populations in Malaysia. *The Qualitative Report, 23*(11), 2700-2713. https://www.proquest.com/scholarly-journals/interview-protocol-refinement-fine-tuning/docview/2151128806/se-2?accountid=14872

Yıldız, I. G., & Şimşek, Ö. F. (2016). Different pathways from transformational leadership to job satisfaction. *Nonprofit Management & Leadership*, *27*(1), 59–77. https://doi.org/10.1002/nml.21229

Yin, R. K. (2015). *Qualitative research from start to finish*. The Guild for Press.

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

Young, W., & Levenson, N. G. (2014). Inside risks an integrated approach to safety and security based on systems theory. *Communications of The ACM*, *57*(2), https://doi.org/10.1145/2556938

Appendix A: Interview Protocol

Date of Interview: _____Code Name Assigned: _____

Interview Script

Introduction of myself to the participant.

Thank participant for participating in the study.

Introduce the research topic and ask if the company is currently undergoing any legal actions surrounding the topic. If yes, the process will end at the time with an explanation on avoiding any risks. If no, the researcher will proceed with the remainder of the interview protocol steps.

Provide a copy of the Informed Consent Form to the participant, review the contents of the form, and allow the participant an opportunity to ask any questions.

Inform the participant of how the interview will be conducted with the use of a cell phone as recording device, note taking with pen and paper, the allowance of necessary breaks and limited interview to no more than 60 minutes.

Inform the participant of the steps that will be used to protect the participants privacy and how the data captured will be protected.

Inform the participant of their rights to withdraw from the study or stop the interview if they desire to do so at their discretion.

Remind the participant that the purpose of the study is to explore strategies in cybercrime prevention used by IT businesses.

Once the participant is ready, the audio will begin and the interview will begin, starting with the first interview question. I will only ask further probing question(s) if needed for clarity. I will ask the participant if they are done with each question prior to proceeding to the next question.

Appendix B: Informed Consent

TITLE OF STUDY
Strategies in Cyber Crime Prevention for IT Businesses

PRIMARY RESEARCHER
Sophfronia Tucker
Walden University – Candidate for Doctor of Business Administration
678 478-7683
Sophfronia@gmail.com

INSTITUTIONAL CONTACT
Institutional Review Board
Walden University
irb@mail.waldenu.edu

INTRODUCTION - PURPOSE OF STUDY

You are being asked to take part in a research study that will provide information to meet the requirements for degree completion. The nature of the research is to capture knowledge from leaders (management and technical leaders) with experience in cyber security and cyber-crime prevention. Before you decide to participate in this study, it is important that you understand why the research is being done and what it will involve. Please read the following information carefully. Please ask the primary researcher if there is anything that is not clear or if you need more information.

The purpose of this study is to understand the experiences of IT professional leaders who have experience in protecting their networks from cyber-crime attacks. The objective is to gain insight on the strategies that are being used to prevent cyber-attacks as well as those strategies that are used to recover from a cyber-attack. The information gained, will also be used as gateway for further research in cyber-crime prevention of IT businesses.

SUBJECT PARTICIPATION

The ideal participants are IT business leaders both management and technical leaders who are responsible for implementing cybersecurity practices that protect their business or other businesses from cybercrime. Participants will have at least 2 or more years of work experience and training in their role.

STUDY PROCEDURES

As a participant in this study, you will be informed of all steps required and expectations via this informed consent document. Participants will be asked questions based upon a pre-determined set of 9 interview questions.

All questions asked will be related to the decisions and work that is performed as it related to cyber-security, network protection, best practices used on the job.

Questions are open-ended which will allow for additional dialogue as needed.
Each interview will last approximately 50 minutes and will be conducted only once. This will be done either in person or virtually based upon the participants needs and comfort level.
A brief follow-up will be conducted to ensure that data has been accurately captured by the participant.

POTENTIAL RISKS

There are no known risks. However, you may decline to answer any or all questions and you may terminate your involvement as a participant at any time if you choose.

POTENTIAL BENEFITS

There are no direct benefits to you for your participation in this study. However, I hope that the information obtained from this study will add to the Body of Knowledge for Cyber Crime Prevention, serve as a platform for future researchers in the field of cyber security and aid in the prevention of cyber-attacks for other businesses. Additionally, I hope that you will finding it rewarding to know that your participation serves as a noble contribution to this area of science.

CONFIDENTIALITY

Your responses to this interview will be anonymous. Every effort will be made by the researcher to preserve your confidentiality including the following:
Assigning code names/numbers for participants that will be used on all research notes and documents.
Keeping notes, interview transcriptions, and any other identifying participant information in a locked file cabinet in the personal possession of the researcher.

CONTACT INFORMATION

If you have questions at any time about this study, or you experience adverse effects as the result of participating in this study, you may contact the researcher whose contact information is provided on the first page. If you have questions regarding your rights as a research participant, or if problems arise which you do not feel you can discuss with the Primary Researcher, please contact the Institutional Review Board.

VOLUNTARY PARTICIPATION

Your participation in this study is voluntary. It is up to you to decide whether to take part in this study. If you decide to take part in this study, you will be asked to sign a consent form. After you sign the consent form, you are still free to withdraw at any time and

without giving a reason. Withdrawing from this study will not affect the relationship you have, if any, with the researcher. If you withdraw from the study before data collection is completed, your data will be returned to you or destroyed.

CONSENT

I have read, and I understand the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I understand that I will be given a copy of this consent form. I voluntarily agree to take part in this study.

Participant's signature _____ Date _____

Investigator's signature _____ Date _____

Appendix C: Pre-Interview Script

Sample Verbiage for Researcher

Hello, my name is *Sophfronia Tucker*, thank you for taking the time to speak with me regarding my research on cybercrime prevention in IT businesses. I am a doctoral student at Walden University, and I am looking for candidates that are willing to share their experiences in the workplace, on how they keep their network secure to either prevent or lesson the harm effects of a cyber-attack. Please keep in mind that your participation would be voluntary. I can also supply you with contact information regarding this study upon request.

Should you agree to become a participant, I would provide you with an Informed Consent form, that provides the protocol for conducting the interview. The Informed Consent will state the purpose of the study, ideal participants, procedures of the study, type of questions asked, benefits, and confidentiality disclosures. Your participation will only be needed once for a few questions that should last less than an hour. The information provided will remain strictly confidential and you will not be identified by your answers. You and/or your company's name will not be disclosed in any way. Data will be compiled as a whole, with no individual responses tied to your name or any identifying information about you. All information disclosed during the interview will be kept secured.

1. Are there any questions that I can answer for you?
2. Would you like to become a participant in this amazing research that will aid in helping other companies become more secure and help combat these insidious acts of cybercrime?

If the participant's response is yes, Researcher responds as follows:
Thank you for agreeing to be a participant. Your time invested is truly going toward a worthwhile cause. I will email you a copy of the Informed Consent form that you will sign as agreement to being interviewed. You may return the form to my email address as indicated on the form.

When will be a good time to reach out to you again to schedule the interview? Do you have a preference to a time and place to complete the interview?

End the conversation by thanking them again for their time and offering your contact information should they need to reach you for anything.

If the participant's response is no, Researcher responds as follows:
Thank you so much for agreeing to speak with me and for your consideration.

Closing: Have a wonderful day!

Interview Questions

What cybercrime prevention strategies do you use to protect your business from a cyberattack?

What kind of cyber-prevention education and training do you provide for your employees on a routine basis?

What is your contingency plan if a cyberattack occurs?

What strategies are most effective in training employees to implement safe cyber-security practices?

What strategies do you use to enforce the use of safe cyber-security practices by your employees when they work from home or off-site?

What procedures do you use to ensure that your cyber-security policies are current?

What strategies have you implemented that are most effective in preventing insider data leakage?

What specific leadership strategies do you use to implement your current cybercrime prevention strategies?

What transformational skills do you use to encourage your employees to adhere to safe cybersecurity practices?

What other information would you like to share regarding cybercrime prevention strategies that IT business leaders use to protect their businesses from cyberattacks?

Ask the participant if they have any relevant documentation or materials that they wish to share that supports the practices that they are currently using or plan to implement.

After the final question has been asked, I will share with the participant the process of member-checking and stop audio recording.

Thank the participant for participating in the study and ensure that the participant has my contact information for follow-up questions. Share with the participant that a copy of the interview transcript will be made available to them for review and approval as part of the member checking process.

Appendix D: Interview Confirmation Email Sample

Greetings Participant Name,
Thank you again for agreeing to take part in my study. This email is to confirm that we will be meeting via phone or Zoom on (scheduled date) at (scheduled time) to conduct the interview regarding my study on Cybercrime Prevention. The interview will be recorded and I will be taking note. Should this meeting time present a conflict, please respond to this email to reschedule another time. Otherwise, I will speak with you soon.

Respectfully yours,
Sophfronia

Appendix E: Theme Research Data Results

Word Identified	Times Referenced
Security	87
Training	73
Access	59
Employees	55
Data	45
Cyber	44
Strategies	42
Environment	33
Email	30
System	30
Company	29
Education	28
Prevention	28
Policies	27
Disaster	26
Attack	24
Business	24
Effective	24
Leader	22
Recovery	20
Awareness	20

Themes and Participant Responses

Theme. SubTheme	Participant Count	Document Reference
Cybercrime Prevention Strategy	All	
Incident Response Plans	PA1, PA3, PA4, PA6	
Policies and Procedures	PA1, PA2, PA3, PA6	Yes (4)
Third Party Vendors	PA1, PA2, PA4, PA%	Yes (1)
Cybersecurity Awareness, Training & Education	ALL	Yes (1)
Effective Leadership	ALL	