Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Christopher Curtis Royal

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. Michael Campo, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Brenda Jack, Committee Member, Doctor of Business Administration Faculty

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

Walden University
2023

Abstract

Strategies for Mitigating Cyberattacks Against Small Retail Businesses

by

Christopher Curtis Royal

MS, Webster University, 2022

BS, Liberty University, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2023

Abstract

Small retail businesses are increasingly becoming targets for social media cyberattacks, often losing profitability when forced to close operations after a cyberattack. Small retail business leaders are concerned with the negative impact of cyberattacks on firms' viability and competitiveness. Grounded in general systems theory, the purpose of this qualitative multiple-case study was to explore strategies retail leaders use to deter social media cyberattacks. The participants were 11 small retail business leaders. Data were collected using semistructured interviews and analyzed using thematic analysis. Three themes emerged: using multiple strategies to deter social media cyberattacks, importance of training regarding cybersecurity best practices, and the need for a contingency plan. A key recommendation is for small retail business leaders to provide employees and customers with training regarding proper cybersecurity protocols. The implications for positive social change include the potential to improve cybersecurity measures and enhance a small business' viability and employment opportunities, positively impacting local communities and tax revenues.

Strategies for Mitigating Cyberattacks Against Small Retail Businesses

by

Christopher Curtis Royal

MS, Webster University, 2022

BS, Liberty University, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2023

Dedication

I would like to dedicate this study to Almighty God and my Savior Jesus Christ. Without you I am nothing. You are my rock and unchanging hand, the calm in the storm. Thank you for everything father, and please remember me in your kingdom. I would also like to dedicate this study to a special teacher that pushed me harder, who took an energetic teenager and saw the best in him. Mrs. Rochelle Arrington, my tenth-grade teacher, thank you for your love, guidance and words of wisdom. Also, I would like to thank 2 special teachers that played a big role in my educational journey, Mrs. Jean Long Slate and Mrs. Susan Comer. Thank you for teaching and giving me a chance to express myself, with all the energy that I had built up inside me! Also, last but not I would like to thank my aunts, Ms. Janet Hood, Mrs. Nancy Royal, and my uncle, Mr. Stanley Royal. I would be remiss not to mention my father, Mr. Sam Royal, I will never forget you. Thank you for making me into man that you could be proud of. I would like to thank my mother, Mrs. Cecelia Royal. Thank you for all your sacrifices. God Bless

Acknowledgments

First, I give all glory to my Lord and savior, Jesus Christ, for not letting me quit and giving me the strength and fortitude to keep pushing. I would like to acknowledge my wife, Veraline Eliott Royal, and my three sons Christopher Curtis Royal Jr., Krishawn Jordan Royal, Christian Jayden Royal, for putting up with me for all the late nights and time missed because of schoolwork. Without all your patience, I would not have been able to achieve this great endeavor! Finally, I want to thank Dr. Michael Campo and Dr. Brenda Jack, for your understanding, guidance, patience, and mentorship as you guided me through this journey. God Bless you both and may he keep you both safe from harm!

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

In many ways, technology enhances individuals' daily lives, especially for those owning and operating small businesses. Organizational leaders tend to use advanced technologies in their firms, which has changed how businesses operate (Wang et al., 2022). Indeed, business technology has advanced the status quo of conventional corporate practices. The effectiveness and price of goods and services, as well as business practices, are impacted by new technologies (Thomson et al., 2022). Small business leaders compete in the 21st century's technologically advanced international e-commerce markets using the internet and computers (Har et al., 2022). Global advances in wireless and wired technologies offer businesses many advantages but can also pose risks (Omolara et al., 2022). Cyberattacks are becoming increasingly common for small and retail businesses to be targeted (Sulaiman et al., 2022). This study addressed a prevalent business problem, namely that social media cyberattacks can negatively affect small businesses' viability and customer retention.

Background of the Problem

Cybercrime is a serious problem impacting businesses and organizations worldwide. Cybercrime is the most prevalent type of cyberattack (Lallie et al., 2021). There was a threefold increase in complaints of data theft by criminal organizations between 2011 and 2018 (Rosati et al., 2019; Snider et al., 2021). Organization leaders reported a 15.1% increase in data breaches and cyberattacks between 2020 and 2021 (Brooks, 2022). Small retail businesses are more vulnerable to cyberattacks than larger enterprises because fewer resources are available to combat them (Chidukwani et al., 2022). In response to the COVID-19 pandemic, leaders of small retail businesses used advanced computing systems and communications to work remotely, communicate, manufacture, and market their products, making them more susceptible to hacking and data breaches (Alzaidi & Agag, 2022; Susanto et al., 2021). A major problem is many leaders of small firms fail to anticipate being targeted by hackers, so they do not prioritize preparing for a cyberattack (Ward, 2022). Thus, small retail businesses are at an especially high risk of cyberattacks.

Small businesses have become increasingly more reliant on online technology. Leaders of small retail businesses increasingly adopt social media for business purposes, which increases the risk of social media cyberattacks. Small retail business leaders frequently use social media to attract and engage customers (S. Chatterjee & Kar, 2020), and have also moved toward selling their products directly to customers on social media platforms (Sombultawee & Wattanatorn, 2022). However, these activities can increase the risk of small retailers' exposure to social media cyberattacks, often leading to an erosion of customer trust and loss of sales (Alzaidi & Agag, 2022). While social media users typically understand the inherent risk to their privacy when using social networking sites, they place substantial trust in retailers that use social media to conduct business (R. Chen et al., 2021). A breach of trust resulting from a social media cyberattack can result in the long-term loss of customers (R. Chen et al., 2021). Thus, small business leaders should understand how to prevent social media cyberattacks.

Preventing social media cyberattacks requires some knowledge of information technology (IT) and cybersecurity. Some small retail business leaders lack the IT skills and resources to adopt the latest cybersecurity advice (Alahmari & Duncan, 2020). To control the rising cybersecurity threats and vulnerabilities associated with technology usage, small retail business leaders frequently lack the necessary procedures (Jahankhani et al., 2022). Personal information loss or a data breach can be costly for any firm (Lloyd, 2020). Leaders of small retailers may find recovering from financial losses caused by cyberattacks to be difficult (Chidukwani et al., 2022). The possible adverse impacts on small retail business leaders are the loss of clients, a breakdown of trust, and decreased revenue (Furnell et al., 2020). Small businesses may not survive the loss of customers due to an erosion of trust resulting from a cybersecurity attack.

Cyberattacks can cause irreversible damage to small businesses. In some cases, a cyberattack could result in a total loss of the business due to unrecovered losses in revenue, legal costs, and a diminished reputation (Kamiya et al., 2021). Specifically, according to Hiscox (2019), the average cost of a digital incident to organizations of all sizes is now $200,000, reflecting the growing severity of cyberattacks’ effects. Six months after being harmed by cyberattacks, 60% of businesses fail (Hiscox, 2019). Mitigating cyber risks requires small retail business leaders to develop innovative multitiered security strategies across personnel, procedures, and networks that guide the businesses’ protection, prevention, and response measures (Keskin et al., 2021). In this section, the focus shifts from a brief overview to a more detailed problem description.

Problem and Purpose

The general business problem was that social media cyberattacks can negatively affect small businesses’ viability and customer retention. The specific business problem was that some leaders of U.S. small business retailers lack strategies to deter social media cyberattacks. The purpose of this qualitative multiple-case study was to identify and explore strategies some U.S. retail leaders use to deter social media cyberattacks. Small retail business leaders require more information to develop the knowledge and skills to effectively deter social media cyberattacks (Kipper et al., 2021). Due to the vulnerability of small retail businesses to cyberattacks via social media and a lack of resources to defend against such attacks, the results of this study could have significant implications.

Studying the problem of small business retail leaders lacking strategies to deter social media cyberattacks can have several implications. Some implications include the development of effective strategies to mitigate such attacks, raising awareness among small business retail leaders, and improving small businesses' financial and legal aspects. Cyberattacks can have substantial economic consequences for small businesses (Lloyd, 2020). Cyberattacks can have legal repercussions, particularly if consumer information is exposed (R. Chen et al., 2021). Additionally, researching this problem can aid in developing efficient methods to avoid cyberattacks on social media (R. Chen et al., 2021). By emphasizing the issue of social media cyberattacks on small retail businesses, the study can raise awareness among company leaders and the general public to implement preventative cybersecurity measures. Leaders can assess the economic impact of cyberattacks and establish a case for investing in cybersecurity solutions by examining the issue. Finally, understanding the legal duties and liabilities in the case of a cyberattack of a business may also be an outcome of the current study. Since many small retail businesses lack sufficient security against cyberattacks through social media, the findings of this study provide insights for cybersecurity improvement and business security and growth.

Population and Sampling

The research population was designed to reflect the demographics and characteristics of small business leaders faced with social-media cyberattacks. Data were collected from 11 purposefully sampled small retail business leaders in the United States who were interviewed using semistructured interviews with open-ended questions designed to elicit their perspectives regarding strategies to deter social media cyberattacks. Participants were selected based on meeting the following inclusion criteria for the study: (a) being over 18 years of age, (b) being the leader of a small retail business in the United States, (c) having used social media to conduct part or all of their retail business, and (d) having demonstrated success in mitigating cyberattacks. Recruitment materials included the inclusion criteria so that participants could self-identify as qualified. A demographic questionnaire was also used for data collection, through which information about each participant was collected. Such information included the number of years in business, the number of years doing business using social media, and economic variables regarding each leader’s small business. I also reviewed company documents provided by the participants for relevant information.

Nature of the Study

I used the qualitative research methodology to answer the research question, as the qualitative research method allows researchers to explore solutions to research problems from the participants’ perspectives. A qualitative methodology provided insights into strategies used to deter social media cyberattacks. According to Creswell and Poth (2018), researchers use qualitative methods to answer questions about people's lives, lived experiences, emotions, behavior, perceptions, and feelings, as well as the overall phenomenon undergoing investigation. Researchers typically use qualitative methods when they have incomplete information about a topic or phenomenon (Levitt et al., 2018). Yin (2018) asserted that qualitative researchers examine how people perceive their social conduct in the context of a phenomenon and real-world events. Since the problem being addressed was that more research was needed regarding the strategies of small retail business leaders to deter social media cyberattacks, a qualitative methodology was most appropriate for the study, as opposed to quantitative or mixed methodological research.

A quantitative approach was not required for this research. Researchers use quantitative methods to evaluate phenomena' statistical nature and find relationships and correlations between variables under examination (Mohajan, 2020). None of the four types of quantitative research methods, namely experimental, descriptive, correlative, and quasi-experimental, were appropriate for this study, because I did not seek to study the cause–effect relationship between variables or look at correlations or relationships between variables (Allan, 2020). Quantitative research is based on numerical responses and does not generally provide insights into the thought, motivations, and drivers of a particular group (Mohajan, 2020), which I aimed to examine in this study. Mixed methods draw from both quantitative and qualitative research designs (Timans et al., 2019), which was not suited to the aims of this study. Based on the lack of a quantitative-based research question, a mixed methodology was not appropriate for this study. A qualitative research method using a multiple case study research design was chosen for the study.

Several qualitative research designs were not chosen for the study for various reasons. For example, a phenomenological approach was unsuitable for this research as this method examines a phenomenon by developing a deep understanding of how individuals behave or react to a particular setting (Moustakas, 1994). Phenomenological studies are based on personal knowledge and participant subjectivity and were unsuitable for this research (Moustakas, 1994). Researchers using grounded theory are concerned with developing a theory; this design was not suited to the current context of this research, which sought to understand how business leaders adjust and react to cybersecurity attacks (Deering & Williams, 2020). Finally, a generic qualitative research design was not appropriate, as researchers use this design when the data and research problem is not centralized to a specific setting or event (Liamputtong, 2019). A case study, on the other hand, entails an in-depth assessment of a single case or event in its actual setting (Yin, 2018). Phenomenological, grounded theory, and generic qualitative research designs were not chosen for the study in favor of a multiple case study research design, described below.

To better understand how U.S. small business leaders recognize social media cyberattacks, a multiple case study was chosen for the research design. This study detailed the methods U.S. small retail business leaders successfully employ to thwart social media cyberattacks. Since single case studies generate valuable insights from a single case (Yin, 2018), this approach was not chosen because I wanted to gain multiple perspectives and opinions from various U.S. small retail business leaders. A multiple case study allows for comparing findings across instances (Yin, 2018). A multiple case study provided more convincing evidence than a single case study regarding successful strategies to thwart social media cyberattacks. Therefore, a qualitative multiple case study research design best suited the current study.

Based on the purpose statement, this study benefited from a qualitative research methodology with a multiple case study design to answer the research question. Qualitative multiple case studies have been used to examine other similar business problems, including the shift of digital technologies in circular economy business models (Ranta et al., 2021), understanding data analytics for manufacturing (Belhadi et al., 2019), and problems with sustainable business practices (Tura et al., 2019). This combination of research tradition and design enabled me to pursue the perspectives of small retail business leaders. The study facilitated and encouraged greater insights into social media cybersecurity and uncovered strategies to deter social media cyberattacks. Scholars such as Creswell and Poth (2018) found that qualitative methods aim to answer questions about people's lives, lived experiences, emotions, behavior, and perceptions, making this method appropriate for the study. This study employed a qualitative multiple-case study research design to answer the following research question.

Research Question

What strategies do some leaders of U.S. small retail businesses use to deter social media cyberattacks?

Interview Questions

1. What has been your experience with social media cyberattacks?
2. What strategies do you use to protect your business from cyberattacks?
3. What is your risk assessment process for cybersecurity?
4. What risk management strategies do you use to identify and evaluate cyberattack risks?
5. Please describe how you respond to cyberattacks.
6. What systems and processes do you use to protect your business from cyberattacks?
7. What are the important systematic interdependencies and feedback loops that impact the quality of your cyber-defense tactics against social media cyberattacks?
8. What employee training strategies do you use for security procedures with electronic devices?
9. What steps would you advise someone in your position to follow if a cyberattack threatened their small retail business?
10. What is your cyberattack contingency plan?
11. Before we conclude the interview, what additional information about cybersecurity strategies would you like to share?

Theoretical or Conceptual Framework

The theory that grounded this study is general systems theory (GST). According to von Bertalanffy (1968), who introduced GST, systems theory focuses more on interrelationships than individual modules. Systems are self-regulatory and self-corrective (Nöth, 2021; von Bertalanffy, 1968). The concepts of von Bertalanffy's GST were further developed by Kuhn (1970). Researchers have argued that science does not follow evolution, but rather follows a methodical course of knowledge expanding to the limits of the existing paradigm and replacing one worldview with another through scientific revolutions (Zhu, 2021). A paradigm shift occurs when one worldview replaces another through scientific revolutions (Zenker & Kock, 2020). Those who apply GST principles tend to work more effectively within organizational structures and can manage people and processes more effectively within broader environments (Buchanan, 2019). Information security systems can be understood effectively using the GST approach (Dias et al., 2022). As such, leaders can use GST to help identify cybersecurity solutions for small retailers selling on social media.

Social media use among small retail businesses has become common in recent years. The increased use of social media makes small retailers vulnerable to cyberattacks (Lloyd, 2020). Leaders of small retailers cannot achieve efficient and secure transactions in the social media selling space without strategies, procedures, ongoing risk assessments, and a review of secure network protocols (Alzaidi & Agag, 2022; Saura et al., 2021; Sembada & Koay, 2021). Using GST, I determined and analyzed effective cybersecurity strategies for small retailers in an evolving environment.

Operational Definitions

Cyberattacks: Invasion of electronic, computer, or network devices by unauthorized individuals to cause harm by modifying, restricting, removing, changing, or stealing private information (Y. Li & Liu, 2021).

Cybersecurity: Cybersecurity refers to the systems, software, and processes in place to prevent or defend against malware and cyberattacks (Lezzi et al., 2018).

Hacking: Hacking refers to the attempt by an unauthorized individual to gain access to another computer's internal network by taking control of network security programs to serve an illegal purpose (Kizza, 2020).

Small retail businesses: Privately owned and operated retail businesses that sell or manufacture goods and have less than 250 employees and up to 41.5 million dollars in annual sales, depending on sector (U.S. Small Business Administration, 2022).

Assumptions, Limitations, and Delimitations

This section provides a description of the assumptions, limitations, and delimitations of this qualitative case study.

Assumptions

Several assumptions were made in this study. In research, assumptions are defined as believing something to be true but not confirming it (Theofanidis & Fountouki, 2018). Considering assumptions and factors for mitigating their risks is essential. According to White (2018), research assumptions are presumptions the researcher holds to be true. Three assumptions applied to this study. First, I assumed that the interviews would elicit sincere responses from the participants, as the interviewees stand to gain nothing from being untruthful. Second, I assumed that the participants were truthful in self-identifying as having successful strategies or recommendations based on their experiences for thwarting social media cyberattacks. Third, I assumed that the data given by the participants were appropriate for analysis under GST. The participants were encouraged to be truthful, as the data were anonymized during the analysis part of the study. Assumptions, alongside limitations and delimitations, are essential to understand to ensure the necessary rigor is applied throughout the study.

Limitations

Researchers should be aware of the limitations of their studies. Some limitations, such as the inherent weaknesses of the study, can impact the results and conclusions of the study (Ross & Bibler Zaidi, 2019). Limitations have implications for threatening a study's internal validity (Ross & Bibler Zaidi, 2019). First, this study could have been limited by a lack of participants who own small retail businesses and have successfully thwarted social media cyberattacks. The second limitation was that data collection could have been delayed or inaccessible due to the lack of availability of selected participants for in-person or virtual interviews. A third limitation was the possibility of participants answering questions in a biased manner. Mitigation efforts to overcome these limitations included having a suitable recruitment strategy, scheduling interviews at mutually convenient times, and ensuring that all participants understand the purpose of the study and their rights to confidentiality during the study. Researchers should be aware of the limitations of their research to recognize the study's weaknesses, whereas the researcher sets delimitations to strengthen the study's parameters.

Delimitations

Several delimitations applied to this study. Researchers can set delimitations to restrict their investigation's parameters and scope (Theofanidis & Fountouki, 2018). This study was delimited to participants who were small retail business leaders that (a) were over 18 years of age, (b) were the leader of a small retail business in the United States, (c) used social media to conduct part or all of their retail business, and (d) had demonstrated success in mitigating cyberattacks. Delimitations improve feasibility while prioritizing the significance of the study.

Significance of the Study

The findings of my study should have a substantial impact since many small retail business leaders are vulnerable to social media cyberattacks and lack the skills and resources necessary to prevent such attacks. Most often, proprietors of small firms lack the cybersecurity safeguards that larger businesses possess (Berry & Berry, 2018). Small companies are typically appealing targets for cybercriminals. Sophy (2021) estimated that 43% of all cyberattacks target small firms, and the repercussions may be highly costly in terms of lost productivity and brand damage. These findings may assist executives of small retail enterprises in establishing efficient defenses against social media cyberattacks. The more significant effects of decreasing cybersecurity threats include safeguarding consumers' privacy and keeping small firms' operational costs stable to avoid raising client prices (Grewal et al., 2020). Based on the current problem and a review of the literature, the findings of this study are significant in improving small retail businesses.

A Review of the Professional and Academic Literature

A professional and academic literature search was conducted using the following keywords: *cyberattack*, *cybercrime*, *cyberattack*, *cyberattack, cyber crime*, *small business cyberattacks*, *social media cybercrime*, *social media cyberattack*, and *social media cyber security.* Several databases were searched including Google Scholar, EBSCO, Emerald Insight, ACM Digital Library, IEEE Computer Society Digital Library, Science Direct, and ProQuest Central. Several journals emerged as key sources of information including *IEEE*, *Computer Fraud & Security*, *Computers & Security*, *Journal of Cybersecurity*, and several business management, small business, and IT resources. The literature review contains 152 sources, 124 of which (82%) appeared in English and were published between 2019 and 2023, and 138 of which (90.8%) were peer-reviewed articles. Of those peer-reviewed articles, five (3.6%) were published greater than 5 years ago and 133 (96.4%) were published in the past 5 years. Books comprised 12 of the sources (7.9%). Two books were published before 2018 and 10 books were published in the last 5 years. The remaining two sources were PhD dissertations published in the last 5 years.

The literature review was guided by GST. The general topics reviewed include GST, cybercrime, cyberattacks, social media cyberattacks, and prevention efforts. An overview of the theoretical framework underpinning this study is presented first. The remainder of the review is then presented, which is structured based on the 11 interview questions that were submitted to participants during the data collection process. The themes of these interview questions include (a) experiences with social media cyberattacks, (b) strategies to protect businesses from cyberattacks, (c) risk assessment processes, (d) risk management strategies, (e) responses to cyberattacks, (f) systems and processes to protect businesses from cyberattacks, (g) important systematic interdependencies and feedback loops, (h) employee training strategies, (i) advice for professionals in similar positions, and (j) cyberattack contingency planning. The literature review concludes with an overview of how the existing literature applies to the existing business problem, followed by a summary of the review.

General Systems Theory

GST was the theoretical foundation of this study. As introduced by von Bertalanffy, system theory emphasizes interrelationships rather than individual modules. A system is self-regulatory and self-correcting (Nöth, 2021; von Bertalanffy, 1968). von Bertalanffy's (1968) GST concept was later developed by Kuhn (1970), who argued that science does not follow evolution but rather follows a methodical course in which knowledge expands to its limits and one paradigm is replaced by another through scientific revolutions (Zhu, 2021). A paradigm shift occurs when a worldview is replaced by another following a scientific revolution (Zenker & Kock, 2020). People and processes can be managed more effectively within broader environments when GST principles are applied (Buchanan, 2019). Information security systems can be better understood using the GST approach (Dias et al., 2022). Leaders of small retailers can benefit from referencing GST theory to develop effective strategies for mitigating social media cyberattacks by addressing their business and customer interactions as an integrated system.

GST employs three distinct concepts. von Bertalanffy (1972) described the concepts as; (a) system units, (b) continuous interconnectivity, and (c) analyzing systems provides an understanding of interconnected systems. System units involve systems science, which explores and theorizes systems across various fields. The second aspect of GST, continuous interconnectivity, was considered in terms of systems technology, which refers to issues that may arise in society and technology due to systems theory. The third concept, involving an analysis of the systems, relates to systems philosophy, which pertains to how we think about and conceptualize systems (von Bertalanffy, 1972). Together, these three concepts form the basis of GST.

The components of GST have been widely applied to research such as this current study. In his work, von Bertalanffy (1972) elaborated on the theory of systems and how those theories could be applied to research. As a result of that description, GST concepts can be applied to a study on cybersecurity and cyberattacks, even though the technology was a long way off after the introduction of GST. I applied this theory to analyze how cyberattacks via social media affect small retailers and how leaders of small retail businesses can respond effectively.

GST Components

Small business retailers’ networks should be reviewed and analyzed to determine any security threats that may prevent retail business success. Typical businesses process information, input, and produce some form of output based on the fundamental principles of GST (Jackson, 2019). Inputs and outputs cross boundaries defined by the system (D. Chatterjee, 2021). von Bertalanffy (1972) acknowledged that organizational leaders should interact with their firms' external environments and that a systemic approach can support businesses in accomplishing their goals and objectives. Open systems are affected by their environment; they either accept inputs from the environment or release outputs from it (Roth, 2019). Researchers can use GST to determine and minimize cybersecurity threats.

The systems referenced in GST are precise. In GST, a system is a collection of parts that interact and depend on one another to form a comprehensive whole (von Bertalanffy, 1972). An environment's boundary describes and separates the system from other systems within the same environment. The extent and pace by which systems that learn and adapt depends on environmental engagement and other organizational contexts (von Bertalanffy, 1972). An organization consists of subsystems interacting in a dynamic environment to accomplish a shared goal; any shift in one subsystem affects the organization (Reimsbach & Braam, 2022; Small et al., 2021). GSTs could promote interdisciplinary cooperation and scientific findings in fields without such theories (Rousseau, 2015). Systems theory applies to a business's management of staff and operations (Rousseau, 2015). GST has been used as a useful framework across multiple studies.

GST can be applied across various sectors and topics of research. In addition to enhancing understanding of organizational relationships, the GST framework is an appropriate grounding for studies on developing strategies to improve an organization (von Bertalanffy, 1972). GST is essential to understand the resilience of social-ecological systems (Van Assche et al., 2019). In their review of GST applications, Van Assche et al.

(2019) examined social, ecological, and adaptive aspects finding that systems theory in interdisciplinary fields has significantly developed post-Bertalanffy. One development is the application of GST to studies on cybercrime.

Another scholar who is well-known for GST work is Vanderstraeten. Vanderstraeten (2019) conducted a thorough review of GST as it has evolved, been applied to research, and examined criticism of the theory that has emerged since it was first introduced in 1968. Vanderstraeten found that new emerging contributions have enriched GST. Vanderstraeten asserted that the concept of a system and its system viewpoint has changed over time in several ways. System viewpoints, however, have also been discredited. The methods of generating knowledge have been contested at various points in history.

According to several academic perspectives, GST is a way of understanding parts of the world based on a system model and reshaping these parts following a system image. This viewpoint is favored by scholars and decision-makers who subscribe to the concept of the system (Rodriguez, 2019). Despite criticism, Vanderstraeten (2019) ascertained that GST’s essential insights are helpful for making a reflexive difference. Our understanding of the modern world has been shaped by the idea of systems, which has also helped shape our understanding of the world (Vanderstraeten, 2019). The structure of the relationship between man and the environment has become central to our efforts to understand the world and has also shaped and reshaped it (Vanderstraeten, 2019). GST is an effective theory in which this research is grounded. In the next section, I will describe the specific ways in which GST can be applied in the field of cyberattack studies. I will include a description of the use of GST to model in the analysis of cyberattack dynamics, which will provide context for the development of effective response strategies used by some U.S. retail executives to deter social media cyberattacks.

Application of GST in Cyberattack Studies

Scholars have applied GST to studies on cybercrime and cyberattacks. D. Chatterjee (2021) addressed discourse regarding whether there is a central artifact that captures the essence of information systems. A study on strategic staffing as a solution to preventing and mitigating the effects of cyberattacks conducted by Hai-Jew (2019) was grounded in GST. Cybersecurity risks are increased due to businesses being either understaffed or staffed with employees lacking the knowledge necessary to develop systems to reduce cyberattack risks (Hai-Jew, 2019). D. Chatterjee analyzed information systems with a heavy focus on the information systems artifact and utilized GST as their conceptual framework. Specifically, D. Chatterjee surveyed 310 firms to understand how small and medium enterprises use social media for marketing. The author found that the impact of social media marketing on small and medium businesses is positively influenced by users' perceptions, functionality, ease of use, and compatibility post-adoption. Leaders of small and medium enterprises use social media marketing despite insignificant facilitating conditions, but cost negatively impacts their use (D. Chatterjee, 2021). Multiple defensive lines across all levels provide thorough defenses by using numerous lines of offense at all layers within a system. Hai-Jew (2019) concluded that leaders should consider the costs and benefits of compromising cybersystems.

Many factors contribute to cybersecurity, including policies, laws, law enforcement, technology, surveillance, and social norms. Another example of GST utilized in cybersecurity research is found in Katina and Keating (2018). The authors developed a framework for improving cybersecurity design by described the interdependence and dynamic nature of systems interacting. Additionally, Patel et al. (2020) stressed that designing the efficient and secure system poses the biggest challenge to maintaining cybersecurity. Utilizing a GST framework, researchers found that the system is intelligent enough to evolve and sustain itself in an optimized state alone (Patel et al., 2020). Cyberattacks are not always complex or unavoidable but result from vulnerabilities that can be rectified quickly and are often preventable (Katina & Keating, 2018). Systems should be flexible and dynamic to self-manage increasingly complex and vigorous threats (Patel et al., 2020). Systems will include agents and software services that gather and monitor data continuously (Patel et al., 2020). By using GST as a framework, researchers can recognize vulnerabilities that can enable businesses to self-manage system security threats.

This qualitative multiple-case study aimed to identify and explore strategies some U.S. retail leaders use to deter social media cyberattacks. Due to the vulnerability of small businesses to cyberattacks via social media, the results of the study could have significant implications. Small retail business leaders require more information to develop the knowledge and skills to deter social media cyberattacks effectively (Kipper et al., 2021). People and processes are managed more effectively in broader environments when GST principles are applied (Buchanan, 2019). GST provides a robust basis for understanding information security systems (Dias et al., 2022). Therefore, GST presented a significant opportunity for understanding effective strategies for small retailers selling on social media when identifying cybersecurity solutions.

Routine Activity Theory

While the GST theory provided an opportunity to generate significant knowledge about information systems, other theories, such as the routine activity theory (RAT), were not chosen for the present study. The RAT was created by Cohen and Felson (1979). This theory revolves around three things: namely a potential offender, a suitable target, and the absence of a guardian (Bottoms & Wiles, 1997). For criminal activity to be realized, all three factors must first coalesce. For example, a potential offender must identify a target that does not have the appropriate security (i.e., a guardian; Bottoms & Wiles, 1997). The RAT can rely on a similar methodology as situational crime prevention (Kitteringham & Fennelly, 2020). Situational crime focuses on the setting where the crime occurred rather than on individuals who commit specific criminal acts. As such, the RAT theory considers all the elements of a crime, and practitioners of RAT tend to assess the context as important in outlining responses.

RAT describes routine activities for both offender and the victim, who in this case are cybercriminals and small enterprises. For example, a cybercriminal could be monitoring specific small businesses via social media looking for opportunities to access their systems or databases. Many small businesses leaders do not effectively secure their networks (Raineri & Resig, 2020), becoming cybercriminals' targets. Network security protocols and other security measures could be vital instruments in preventing crime.

Without access or controls in security systems, firms can become potential targets. In normal situations, guardians could range from network security professionals to hacking alarm systems, or in corporate contexts, guardians can range from processes, software, or other authentication steps designed to prevent intruders (Perwej et al., 2021). Establishing preventive programs that are designed to protect employees via security and safety training is crucial in cybersecurity, as well as procedures and technologies that are suited to individual contexts.

RAT was not appropriate for this study for numerous reasons. First, capable guardians under the RAT generally take the form of physical persons such as IT professionals (Shoenberger, 2021). However, many small businesses do not have a separate IT or cybersecurity department (Ahmad & Thurasamy, 2021), leaving the small business leader to operate the IT department and manage the company. Many small business leaders need to fully understand the depth of cybersecurity (De Kimpe et al., 2018), rendering the guardian ineffective under RAT. Meanwhile, GST is driven by an understanding and a dissection of information systems, enabling businesses to understand the nature, type, and severity of cyberattacks.

I did not utilize RAT in this study due to the main criticism of the theory. A primary criticism asserted by scholars is that criminals tend to be rational in their decision-making (Charmet et al., 2022). The rationale is that cybercriminals may differ from the person implementing security measures, making it difficult to compare and analyze criminal actions and company reactions. The use of RAT would not allow for the consideration of situational crime prevention techniques that are put into effect or may prevent the worst effects of a cybersecurity crisis. Unlike RAT, GST places profound emphasis on people and systems, accounting for the context and types of cybercrime, unlike RAT. GST also accounts for the lapses in human capital and knowledge frameworks, thereby providing a more comprehensive understanding of cyber-crimes' nature (Hai-Jew, 2019). I chose GST because systems theory is an appropriate framework for the study. Drawing on this theoretical framework, the remainder of this literature review contains a synthesis of literature related to the interview questions that I asked participants during the data collection phase of my research.

Experiences With Social Media Cyberattacks

Cybercrimes are a pervasive problem, especially following COVID-19. Cybercrimes are unlawful acts conducted through the internet (Al-Khater et al., 2020) and are highly prevalent (Lallie et al., 2021). The number of complaints of data theft by criminal organizations tripled between 2011 and 2018 (Rosati et al., 2019; Snider et al., 2021). Specifically, data indicate that cybercrimes have been more prevalent following the 2020 COVID-19 outbreak (Monteith et al., 2021). There was an increase in data breaches and cyberattacks of 15.1% in 2021 as compared to 2020 (Brooks, 2022). The data show an increase in cybercrime may cause significant repercussions for society.

Social media cyberattacks are of immediate concern for small retail businesses. Small businesses suffer disproportionate repercussions of social medial cyberattacks (Baier, 2019). Specifically, various businesses use social media to communicate with their clients, vendors, and customers (Baier, 2019). A systematic review of the literature on cyberattacks originating from social media was conducted by Wilbanks (2020).

Wilbanks emphasized the importance of social media for businesses to initiate communication with customers and generate revenue. S. K. Khan et al. (2020) identified social media messaging as one of the top ten most concerning cybersecurity threats to emerge during the COVID-19 pandemic. Leaders of small retailers frequently use social media to reach and engage their customers (S. Chatterjee & Kar, 2020). Social media platforms have also become popular for small retail businesses to sell their products directly to customers (Sombultawee & Wattanatorn, 2022). These activities can expose small retailers to social media cyberattacks, which often erode customer trust and lead to loss of sales (Alzaidi & Agag, 2022). The use of social networking sites involves an inherent risk to privacy. Consumers place great trust in retailers that use social media for business (R. Chen et al., 2021). If a cyberattack on social media breaches that trust, leading to long-term customer loss (R. Chen et al., 2021). Social media cyberattacks pose risks to small retail businesses and their customers; however, there are some measures leaders can use to prevent or minimize cyberattacks.

Small retail business leaders tend to use social media to predict customer behavior; therefore, a social media cyberattack could harm businesses and decrease customer trust. Based on quantitative data, Alzaidi and Agag (2022) developed a model of consumers' purchase behavior in social media influenced by trust and privacy concerns. According to the authors, purchase intention depends on trust, privacy, and security concerns. These findings provide important information regarding consumers' shopping habits through social media and what can influence them to either shop with a particular retailer or choose a different retailer. The authors ascertained that customer attraction and retention could be impacted by social media cyberattacks. Additionally, Susanto et al. (2021) explored digital social media security trends and usability during COVID-19. The authors' findings revealed that many businesses took advantage of different features of social media during the pandemic. The authors also highlighted the importance of businesses maintaining a positive online presence. Susanto et al. asserted that small businesses could communicate with customers through social media, including WhatsApp, Telegram, Zoom, Microsoft Team, and Edmodo. Susanto et al. indicated that social media improved businesses' security and usability during the COVID-19 pandemic. Working from home, setting up a new company, and improving business processes were among the factors examined. These findings indicate the importance of social media for small businesses and outline the necessity of protection against cyberattacks.

Current research about social media cyberattacks in the retail sector analyzes how working from home, establishing a start-up, improving business processes, and conducting online business impact the cybersecurity of small retail businesses. Saura et al. (2021) examined the ethical implications of the design elements of social media platforms intended to influence user behavior. In this review, the authors examined how performance metrics can be used to assess the efficiency and ethical concerns associated with such design elements. Previous studies have emphasized the significance of ideas like ethical design in social network systems since users may not be aware of being influenced in digital marketplaces through advertising, information architecture design, or behavior prediction (Zuboff, 2019). According to Saura et al., three primary performance metrics were developed to evaluate the effectiveness of design elements aimed at changing user behavior in social media: engagement, influence, and persuasion. Engagement is the measure of how users interact with content and services on a platform. Through their own behavior, individuals can influence the behavior of others on the platform (Saura et al., 2021; Zuboff, 2019). As a result of exposure to information or features on the platform, users' beliefs or actions may change and businesses will have to keep up with such features.

Cyberattacks can have major implications, such as financial losses, reputational harm, and compromising sensitive personal or corporate information (Azubuike, 2021). To reduce the dangers of social media cyberattacks, people and organizations should be aware of the strategies attackers use and make proactive efforts to defend themselves. Techniques to reduce cyberattacks include regular assessments of the cybersecurity of small and medium businesses and conducting internal and external audits, using strong passwords, activating two-factor authentication, and keeping software and security procedures up to date (Devi, 2023). By adopting these best practices, individuals and organizations may dramatically lower their chance of falling victim to a social media hack (N. A. Khan et al., 2020). In the following section, I will describe numerous preventative techniques that can assist people and organizations in defending against social media cyberattacks.

Strategies to Protect Businesses From Cyberattacks

Cybersecurity is an issue that small businesses should address. Small businesses have become more vulnerable to malware infections due to adopting new technologies

(Coburn et al., 2018). Kakucha and Buya (2018) described that small businesses should use systems designed to provide confidentiality, maintain integrity, and safeguard privacy. An effective cybersecurity approach for small retailers should provide resilient, adaptable security (Alawida et al., 2022). Small retail businesses require effective strategies to minimize cyberattacks (Alawida et al., 2022). Managing critical infrastructure, safeguarding public safety, and protecting consumer data are all vulnerable to cyberattacks (Ding et al., 2018). Small retail businesses leaders should upgrade or invest in new technology to improve their cybersecurity.

Cybercrime has disproportionally and negatively affected small retail businesses in wake of the COVID-19 pandemic. Cyberattacks are more likely to affect small retail businesses than large corporations because they have fewer resources to defend against them (Chidukwani et al., 2022). Leaders of small retailers have used advanced computing systems and communications to work remotely, communicate, manufacture, and market their products in response to the COVID-19 pandemic, making them more vulnerable to data breaches and hacking (Alzaidi & Agag, 2022; Susanto et al., 2021). Leaders of small firms typically do not prioritize preparing for a cyberattack because they do not anticipate being targeted by hackers (Ward, 2022). N. A. Khan et al. (2020) studied the increased use of technology following social-distancing requirements imposed due to the COVID-19 pandemic. The authors emphasized that due to the increasing use of universal computing, cybersecurity threats are also increasing due to the world and technological advances. Khan et al. identified the top ten most severe cybersecurity threats: malicious social media messaging, spam emails, business email compromise, mobile applications, browsing applications, DDoS attacks, malicious domains and websites, malware, and ransomware, which can negatively affect small businesses. In the wake of COVID-19, small businesses were greatly affected by the increase in cybercrime and are also targets for cyberattacks.

Cybercriminals and hackers can disrupt small businesses' networks. Cyberattack refers to hacking that affects a computer network or a computer-linked device (Kaushik et al., 2021). The mismanagement of network technology can result in cyberattacks (Liu et al., 2020). Cybercrime poses an ongoing threat to small retail businesses. By using malicious code, cybercriminals can cause damage to computer codes and data, which can lead to crimes such as identity theft and data theft (Alazab et al., 2021). Additionally, social media-based cyberattacks have significantly increased during the second decade of the 2000s (Alzaidi & Agag, 2022). As cyberattacks increase in frequency and sophistication, business leaders should create or adopt security plans to prevent security breaches (Afaq et al., 2023). Cyberattacks significantly disrupt networks that small retail businesses use to continue operations.

Using performance metrics to manipulate user behavior for commercial or other purposes may be misleading. For example, social media platforms may use design elements to boost engagement or influence to attract users or generate more advertising revenue, even if these features negatively affect users' well-being or autonomy (Saura et al., 2021). The authors also advocated for more research on the ethical implications of social media design elements that try to influence user behavior. Sembada and Koay (2021) investigated the association between perceived behavioral control (PBC) and trust in the setting of social media shop purchases. PBC refers to an individual's belief that they have control over their own conduct and is a key predictor of trust in online purchase scenarios. Researchers concluded that social media platforms should be designed with additional ethical considerations, such as using more transparent and respectful performance metrics to measure user autonomy and well-being (Saura et al., 2021; Sembada & Koay, 2021). The authors surveyed consumers who bought from social media retailers and discovered that PBC was highly associated with trust (Sembada & Koay, 2021). The scientists also discovered that PBC moderated the association between trust in the shop and future purchase intent. Improving PBC and reducing cyberattacks may aid in building trust and encouraging future purchases from small retail businesses.

Small Retailer Cyberattack Susceptibility

Small retailers are susceptible to cyberattacks which puts customer privacy at risk. Leaders of small retailers commonly use social media to engage with their customers and attract new ones (S. Chatterjee & Kar, 2020). Social media platforms have become increasingly popular among small retail businesses, especially following the 2020 COVID-19 pandemic (Sombultawee & Wattanatorn, 2022). As a result of these activities, small retailers are more likely to be exposed to social media cyberattacks, which can erode customer trust and decrease sales (Alzaidi & Agag, 2022). The use of social networking sites entails inherent privacy risks for social media users. In order to conduct business, retailers should trust their customers (R. Chen et al., 2021). In the event of a social media cyberattack that breaches that trust, long-term customer loss may result (R.

Chen et al., 2021). Social media cyberattacks threaten small retail businesses and for some businesses it is a challenge to maintain preventative cybersecurity measures.

Small business leaders need to protect their firms' social media accounts against cyberattacks as customers engage with the accounts frequently. Yaokumah et al. (2020) ascertained that small businesses need help protecting their infrastructure against cyberattacks. Only 20% of small and medium-sized businesses have implemented policies for preventing and responding to cyberattacks (Nobles & Burrell, 2018). Organization leaders have been motivated to develop cybersecurity plans due to recent cyberattacks to assist them in formulating strategic visions and risk assessments (Falco & Rosenbach, 2022). There are many ways in which business customers engage with brands and create relationships with firms using social media (Sombultawee & Wattanatorn, 2022). Customer brand engagement is influenced by information quality and rewards, and by selling products on social media. Social selling plays an important role in the engagement of customers with brands, and privacy and security concerns play a role in customer brand engagement as well (Sombultawee & Wattanatorn, 2022). The evidence regarding small business cyber infrastructure and social media engagement with customers supports the current study on how cyberattacks impact small business operations.

Small retail businesses need to improve in terms of employee technology training. Unger (2021) found that small and medium businesses are more susceptible to cyberattacks than larger companies due to limited employee training, the absence of in-house IT professionals, budget constraints, and inadequate cybersecurity defense and response plans. The most common type of cyberattack experienced by small businesses is phishing, with 75% of global companies reporting a phishing attack in 2020 (Unger, 2021; Vincent, 2019). The COVID-19 pandemic has also increased cyber threats due to the transition to remote work and insecure IoT devices and home networks. Vincent (2019) also posits that small businesses underestimate the cyber threats they face, are underfunded in cybersecurity, and need more knowledgeable cybersecurity personnel to assist them in preparing and defending against attacks. Small business leaders should improve employee training in cybersecurity awareness in order to reduce cybersecurity threats.

Small retail businesses are particularly susceptible to cyberattacks due to their limited resources and need for cybersecurity expertise. These attacks can have significant financial consequences for small retailers, including the cost of responding to the attack and the potential loss of customers (Kusumastuti et al., 2020). Small retail businesses can incur high costs due to cyberattacks, including direct costs such as financial losses and indirect costs such as responding to and recovering from an attack (Tam et al., 2021). These costs can harm a small retail business’s financial stability and success due to reduced trust (Z. F. Chen & Cheng, 2020). In the next section, I will describe the measures that small retail business leaders can take to prevent cyberattacks and mitigate the associated costs. I will also examine the costs associated with cyberattacks on small retail businesses in more detail.

Risk Assessment Processes

Businesses and individuals should take more precautions as cybersecurity threats increase in frequency and sophistication, and the first step in managing risk is to assess the economic risk and potential impacts that may result from a cybersecurity breach. Leaders should be proactive to prevent cyberattacks, especially when attacks are repeated (Alawida et al., 2022). Business leaders should prioritize data security to sustain their businesses in the long run (Ghelani, 2022). Hackers use numerous methods to intercept private data, including spending millions of dollars on behalf of clients and creating weaknesses in client accounts (D. Chatterjee, 2021). Lloyd (2020) described the business benefits of cybersecurity for small and medium businesses. The author concluded that small and medium businesses could be more cyber-ready by having regular assessments of the cybersecurity of small and medium businesses and conducting internal and external audits (Lloyd, 2020). Factors regarding cybersecurity issues in small and medium businesses included customer retention. The recommendations made by the author could serve as a framework for the interviews the researcher will perform to guide thoughts about cybersecurity related to social media cyberattacks (Lloyd, 2020). Small retailer business leaders can mitigate these cyber threats by taking several preventative measures, despite the challenges associated with countering monumental efforts by cybercriminals.

If a small retailer or business does fall victim to a cyberattack, the firm could suffer financially. Small retailers may not recover from financial losses caused by cyberattacks (Chidukwani et al., 2022). Cybersecurity defense expenses are increasing due to the damage cyberattacks cause (L. Li et al., 2019). Some of the possible adverse impacts on small retail business leaders is the loss of clients, a breakdown of trust, and decreased revenue (Furnell et al., 2020). These findings are true regarding traditional cyberattacks and those that stem from social media. Additionally, Hiscox (2021) surveyed 590 U.S. small businesses. According to the survey, approximately 23% of small businesses surveyed have suffered cyberattacks in the past 12 months. Notably, on average, U.S. small businesses are costing $25,612 over 12 months due to cyberattacks. However, other scholars warn that the actual costs of cyberattacks are challenging to estimate due to many undiscovered cyberattacks (Alahmari & Duncan, 2020). Financial loss may be a consequence of cyberattacks, but there are marketing strategies that can be used to increase business profitability.

Social media marketing can help improve small business profitability. Many factors could aid small and medium businesses in implementing social media marketing methods to increase their profitability (S. Chatterjee & Kar, 2020). For example, social media marketing positively impacts small and medium businesses (Schaupp & Bélanger, 2014). Perceived usefulness was identified as one of the factors, and perceived ease of use and compatibility as the second (S. Chatterjee & Kar, 2020). Small and medium businesses increasingly adopt social media marketing (S. Chatterjee & Kar, 2020). A social media marketing strategy is important for small businesses (Schaupp & Bélanger, 2014). Small retail businesses are vulnerable to social media cyberattacks due to social media marketing (S. Chatterjee & Kar, 2020). Technology and social media perceptions of company members may influence companies' strategies to protect themselves from social media attacks.

Cybercrime can cost small businesses significant financial damages. In a study by Anderson et al. (2019), the authors described the issues and approaches for calculating the cost of cybercrime and its impact on businesses. The authors examined the many costs of cybercrime, including direct costs like revenue losses and indirect costs like reacting to and recovering from an attack. Anderson et al. described the shortcomings of current approaches for calculating the cost of cybercrime, such as the difficulties of precisely assessing intangible costs like reputational harm and the impact of cybercrime on productivity. The authors explored the financial losses that retailers might sustain due to cyber assaults, both the direct cost of the attack and the indirect expenses involved with recovery. Anderson et al. also described that cyber assaults may negatively influence a company's reputation and consumer loyalty, resulting in additional revenue loss. According to the authors, precisely calculating the cost of cybercrime is critical for organizations to handle and avoid it successfully (Anderson et al., 2019). The changing nature of cyber threats and the evolving impact of cybercrime on organizations requires leaders of small retail businesses to define new approaches to measuring cybercrime's cost.

During COVID-19, an increased risk of cyberattacks occurred due to the widespread use of remote work and online communication tools. For example, Muheidat et al. (2020) described the use of data analysis to predict and prevent cyberattacks during the COVID-19 pandemic. The authors described the use of data analysis and a proposed secure Internet of Things (IoT) layered model to predict and prevent cyberattacks that may occur during the COVID-19 pandemic. Indeed, the researchers propose a layered model for securing IoT devices that includes multiple security measures such as encryption, authentication, and firewall protection (Muheidat et al., 2020). The authors also demonstrate the use of data analysis techniques to identify patterns and trends in cyberattack data, which can help predict and prevent future attacks. Pranggono and Arabo (2021) found that as cybercriminals become more aware of the situation, it becomes much easier for them to create false messages or websites that appear to be affiliated with well-known authorities, using words like urgency to capitalize on the widely felt fear factor associated with handling an emergency and meet needs. When the most susceptible individuals are more nervous and anticipate emails, texts, calls, etc. pertaining to COVID-19 from the authorities, these frauds are considerably more successful currently during the epidemic.

Risk Management Strategies

When leaders access corporate funding to upgrade their cybersecurity systems, their firms become more resilient. There is a significant gap in small businesses' cybersecurity efforts because many small business leaders do not perceive their companies as cyberattack targets (Espinosa, 2022; Raineri & Resig, 2020). Companies are becoming unsustainable because of rising cybersecurity costs, a trend not likely to subside in the foreseeable future (Shaverdian, 2019). Today's technological era is changing how people connect to the world, resulting in a desire for constant, immediate connectivity (Caboni, 2020). For example, the internet drives innovation, growth, and competitive advantage globally and nationally (Lee & Falahat, 2019). As a result, a new retailer has emerged in the retail sector, providing customers with an immersive, digital shopping experience. Caboni (2020) ascertained that for retailers to achieve this immersive experience, connectivity, authenticity, and style should be prioritized. Connectivity refers to the ability to send and receive large amounts of data instantly and globally and is connected to the new kinds of relationships developed through digital technologies (. Authenticity refers to the desire of people to connect with real, authentic individuals, particularly during their shopping journey. With the use of funding or investment into digital technologies utilizing connectivity and authenticity, small retail businesses can improve their cybersecurity.

Improving knowledge and education about cybercrime and fraud prevention might help reduce financial risks for online customers. Siahaan and Nasution (2018) described the prevalence and impact of cybercrime and fraud in online shopping, including the financial losses that can result from these crimes. These crimes can cause direct financial losses for online buyers, such as unlawful credit card usage or the loss of personal cash due to a hoax (. The researchers also explored the indirect financial impact of cybercrime and fraud, such as the expense of recovering from an attack and the possible loss of company or job chances due to reputational harm. Corallo et al. (2020) examined the significance of cybersecurity in the context of Industry 4.0, the present trend of automation and data interchange in industrial technology, and the possible consequences of cyber assaults on organizations. Corallo et al. (2020) explained that customers may lose faith in the security of a company’s products or services and the protection of personal data due to cyber assaults. The authors claim that trust is critical for a company’s performance and that strong cybersecurity measures are required to prevent cyber assaults from jeopardizing confidence. Cyber assaults can cause stakeholders to lose faith in a company's capacity to secure its assets and keep critical information private.

Small Retailer Cyberattack Prevention

There is an increasing number of cyberattacks targeting small retail businesses, which can potentially cause significant damage to the company and its customers. Tao et al. (2019) explained that the loss of sensitive data, revenue loss, and trust erosion can all result from these cyberattacks. Small retail businesses should therefore take proactive measures to prevent cyberattacks and protect their operations (Okereafor & Adelaiye, 2020). Implementing a holistic cybersecurity strategy is essential, which includes identifying possible risks, training staff, and regularly monitoring and upgrading security protocols (Stewart, 2022). A multifaceted and varied approach to cybersecurity is necessary to effectively prevent and mitigate the effects of cyberattacks.

Software and Technology

As technology develops and cyberattacks become more sophisticated, small retail businesses should adopt new security measures. Additional security measures are necessary to protect company data, assets, and intellectual property (Alawida et al., 2022; Sanders et al., 2022). Small retailer leaders should address their primary weaknesses in business practices, systems, and cultures when implementing software applications to prevent or deter cyberattacks (Temel & Durst, 2020). Business leaders have increasingly adopted technology to maintain security within their organizations (Satterfield et al., 2018). Firewalls can also prevent server attacks by filtering malicious traffic (Kantheti &

Manne, 2022). Using modern technology in small businesses is crucial for preventing cyberattacks.

Small businesses leaders should work to secure new products and services to address online cybercriminals. A firm that lacks an actionable software inventory is more likely to be attacked (Kantheti & Manne, 2022). Organization leaders tend to use a variety of software programs to identify problems and resolve them (Alluhaybi et al., 2019). Although these programs can be effective, developing or adopting security software is often challenging, inconvenient, and prohibitively expensive (Paquet-Clouston et al., 2018). This is part of the reason that small retailers with fewer resources than large retailers are often at higher risk for cyberattacks (Alahmari & Duncan, 2020). Small businesses are at a greater risk for cyberattacks due to a lack of new technological services to prevent attacks.

Email Security

Small retail business leaders should invest in email security to protect their firms, employees, and customers from email security risks. Email technology is indispensable to most businesses (Lallie et al., 2021). Email is often used to send malware, spam, and phishing attacks (Yu, 2020). Email security involves developing and implementing policies or procedures for protecting email accounts, content, and communication against unauthorized access, loss, or compromise (Al-Musib et al., 2021). Small retailers leaders may opt to implement aggressive spam filtering, so malicious and spam emails do not appear in the user's inbox (Mohammad, 2020). Employees should equally be aware of various types of spam and should impose mandatory training to enable them to recognize spam (Cross & Gillett, 2020) Furthermore, small retail businesses have had success in preventing email cyber and server attacks by leveraging firewalls to filter malicious traffic (Permana et al., 2022). Heightened email security is imperative for small businesses to avoid spam and phishing scams.

Cyber Insurance

Cyber insurance can cover unexpected costs associated with cybercrimes. Cyber liability insurance is a good way for small retailer leaders to protect their firms from breaches (Gunduz & Das, 2020). Many companies purchase cyber liability insurance policies to protect themselves from cybercrime or data breaches (Lemnitzer, 2021). Due to their reliance on the internet and network structures, small resilience businesses purchase cyber liability insurance (Lu et al., 2018). In the event of service outages, cyber insurance will provide businesses with financial compensation (Lu et al., 2018). Cyber insurance can offer small businesses protection; however, there are risks that extend to the customers.

Businesses and customers can be affected by cyberattacks, but customers are not always covered by cyber insurance. According to Patterson (2020), cyber insurance requires regulation. The authors ascertained that cyber insurance should be a requirement for businesses due to the potential cost barriers of making reparations in case of a breach. When a breach of personal information or privacy, cyber insurance covers the business' legal fees and expenses, notifies its customers about the breach, restores the identity of the affected customer, recovers the compromised data, and repairs the business' computer systems (Lu et al., 2018). When there is a breach of personal information, most states require companies to notify their customers, which can be expensive (Lemnitzer, 2021). Similarly, even if credit monitoring is not required in most states, such a gesture can go a long way in maintaining goodwill (Franke & Meland, 2019). Depending on the state, the customer is required to be notified in the case of a cyberattack, but in some states, this is not required which in turn compromises the customer's privacy.

Routine Audits

To prevent assets from being compromised, business leaders should conduct routine audits. For example, web applications should be audited for security issues, and any issues should be immediately addressed (Imtiaz et al., 2021). A study carried out by Lloyd (2020) described the benefits of cybersecurity for small and medium businesses. Regularly assessing a small or medium business's cybersecurity and internal and external audits can help firms become more cyber-ready. As a result of performing these four tasks regularly, small retailers will be more cyber-ready to engage with customers online. Lloyd (2020) described factors involved in addressing cybersecurity issues in small and medium businesses, including ways to retain customers in the face of cyberattacks. The recommendations made by the author could serve as a framework for the interviews the researcher will perform to guide thoughts about cybersecurity related to social media cyberattacks.

Ethical Strategies

Strategies for combating social media cyberattacks should prioritize ethics. Kilgour (2020) found a link between users' privacy concerns in digital environments and ethical design. Businesses should be intentional in their efforts to protect their customers from privacy breaches (Kilgour, 2020). When a business's ethics are questioned, customers become increasingly concerned about their data privacy (Hayes & Kelly, 2018). Christen et al. (2020) analyzed the ethical challenges that emerge in cybersecurity, such as privacy, consent, trust, and responsibility. The authors described the significance of ethics in cybersecurity policy and practice and the difficulties of creating ethical frameworks that can successfully handle cyber threats' complex and rapidly shifting nature . Ethical standards should be applied to all elements of cybersecurity to guarantee that the technology is utilized responsibly and in the best interest of all parties.

Small retail businesses are increasingly targeted for cyberattacks, which can have significant consequences for both the business and its customers. Therefore, small retail businesses should take proactive measures to prevent cyberattacks and protect their operations (Udofot & Topchyan, 2020). Preventing cyberattacks is crucial for an organization's security and success. By implementing strong cybersecurity measures and training employees to identify and mitigate potential threats, businesses can significantly reduce the risk of cyberattacks and protect sensitive data (Tam et al., 2021). However, leaders of small retail businesses should recognize that cybersecurity is an ongoing process and requires continuous monitoring and updates to stay ahead of evolving threats (Puławska et al., 2022). Small retail businesses should also prioritize cybersecurity to protect their assets and customers. In the next section, I will address cybersecurity for small retail businesses and how they can effectively address these cybersecurity challenges to ensure the security of their operations.

Responses to Cyberattacks

Due to their limited resources and less stringent security measures compared to larger organizations, cybercriminals increasingly target small businesses. There is evidence that small businesses are not adequately prepared to respond to cyberattacks, and as a result, they frequently suffer significant consequences. According to one recent report, 28% of cyberattacks targeted small enterprises (Ncubukezi, 2023). This statistic indicates that cybercriminals frequently target modest businesses. According to another study, 66% of small businesses encountered a cyberattack and 63% experienced a data breach in the previous year (Y. Li et al., 2020). Despite these high numbers, only 28% of the small businesses surveyed deemed their ability to prevent cyberattacks to be highly effective. In the same study, the average cost of a data breach for small businesses was determined to be $200,000. The high cost of cyberattacks can be especially detrimental to small businesses, with some unable to recover and being compelled to close.

Lack of resources may contribute to the incidence of cyberattacks among small businesses. Small businesses frequently have limited budgets, which prevents leaders from investing significantly in cybersecurity measures, such as hiring IT specialists or purchasing advanced security software (Gulyas & Kiss, 2023). This dearth of resources and knowledge increases their susceptibility to cyberattacks. According to one recent study, more than half of small business leaders believe that their employees are the weakest link in their cybersecurity efforts (Franck & Reith, 2022). This emphasizes the need for improved employee training and awareness programs to reduce the likelihood of cyberattacks.

Some small businesses leaders only implement cybersecurity measures in response to cyberattacks, rather than as part of daily operations. Small business leaders frequently take a reactive rather than proactive approach to cybersecurity, addressing issues after they have occurred (Buresh & Esq, 2022). This strategy may result in more extensive damage and increased expenses. Adopting a proactive strategy, such as undertaking routine risk assessments and implementing security best practices, can aid in mitigating the effects of cyberattacks (N. A. Khan et al., 2020). Small businesses can benefit from collaborating with other organizations and industry groups to improve their cybersecurity measures by sharing knowledge and resources. For instance, the National Cyber Security Alliance (NCSA) provides small businesses with resources and support to enhance their cybersecurity posture.

Small businesses are at an increased risk for targeting by cybercriminals. There is substantial evidence to suggest that, due to limited resources and expertise, small businesses are at a greater risk of cyberattacks (Franck & Reith, 2022; Y. Li et al., 2020; Udofot & Topchyan, 2020). This, coupled with the financial repercussions of such assaults, underscores the need for small businesses to adopt a more proactive approach to cybersecurity, invest in employee training, and collaborate with other organizations to strengthen their defenses (Franck & Reith, 2022). The following section contains a review of the literature associated with systems and processes to protect businesses from cyberattacks that may occur.

Systems and Processes to Protect Businesses from Cyberattacks

Systems and processes to protect businesses from cyberattacks begin with organizational leaders, who should develop skills needed to understand how to most effectively manage any risks that exist. Due to the large amount of business done online, small retail business leaders should develop and maintain social media competencies (Devi, 2023). If a threat gains access to a company's internet, the company could suffer financial ruin, relationships may be damaged, and growth and development can be slowed down (Wilbanks, 2020). Kipper et al. (2021) conducted a systematic literature review regarding the interpersonal and adaptive competencies business leaders require to remain abreast of emerging cybersecurity protocols. The authors suggested a set of knowledge and skills that must be developed to stay relevant in the new global digital "Industrial Revolution." Using a general systems approach, Kipper et al. (2021) analyzed the knowledge and skills required to keep up with cybersecurity and cyberattacks. Kipper et al. provided insights into the knowledge and skills required to keep up with cybersecurity and cyberattacks using a general systems approach. Additionally, Wilbanks (2020) provided information about the importance of social media for small businesses and how these small enterprises should also be aware of the risks involved, including cyber threats. Wilbanks explained that social media threats may be unavoidable, but small business leaders could reduce the likelihood and impact of these threats. Small business leaders should understand how to minimize and mitigate social media risks.

Important Systematic Interdependencies and Feedback Loops

Organizations tend to rely on a set of interdependent systems with feedback loops to conduct their daily operations. Leaders of small retail enterprises who understand and address systemic interdependencies and feedback loops are better prepared to prevent cyberattacks against small retail enterprises (Buresh & Esq, 2022). These interdependencies and feedback cycles frequently involve interactions between people, processes, and technology, making it imperative for businesses to adopt an all-encompassing cybersecurity strategy (Azubuike, 2021). Employees play a crucial role in preventing cyberattacks. A well-informed and trained personnel can assist in identifying potential threats and avoiding phishing email scams (Y. Li et al., 2020). Continuous training and reinforcement of best practices generate a positive feedback cycle that enhances the enterprise's overall security posture.

Ensuring that software and components are current is essential for preventing cyberattacks. Regular updates repair vulnerabilities that could be exploited by hackers. Investing in security tools such as firewalls, antivirus software, and intrusion detection systems can create a feedback loop in which enhanced security measures deter potential attacks and encourage additional investment in security infrastructure (Ncubukezi, 2023). Having a well-documented incident response plan enables small retail businesses to respond quickly and effectively in the event of a cyberattack (Tam et al., 2021). This proactive approach can reduce the potential impact of an attack and expedite the organization's recovery (Puławska et al., 2022). A successful response to an incident can reinforce the significance of thorough planning and lead to the plan’s continual enhancement.

Routine risk assessments enable businesses to prioritize their cybersecurity efforts by identifying potential threats and vulnerabilities. The feedback loop created by addressing identified risks and continuously monitoring for new threats enables businesses to remain ahead of emerging cyber risks (Bahadoripour et al., 2023). Small retail businesses can benefit from sharing knowledge, resources, and best practices with other businesses, industry organizations, and law enforcement agencies (Devi, 2023). This collaboration can generate a positive feedback loop in which shared information leads to enhanced industry-wide security measures, making it more difficult for cybercriminals to succeed.

Maintaining a robust security posture can increase customer confidence and safeguard the company’s reputation. When customers believe a company will manage their information securely, they are more likely to continue doing business with that company. This positive feedback loop can encourage businesses to invest more in cybersecurity measures in order to maintain customer trust (Gulyas & Kiss, 2023). Small retail business leaders should adhere to various regulations and standards, such as the Payment Card Industry Data Security Standard, which regulates the handling of credit card information (Y. Li et al., 2020). Compliance with these standards can result in a positive feedback loop in which meeting regulatory requirements leads to enhanced security measures, thereby reducing the risk of cyberattacks.

Understanding and addressing a variety of interdependencies and feedback cycles is essential to preventing cyberattacks against small retail businesses. These include employee training, technology investments, incident response planning, risk assessment, collaboration, client trust, and compliance with regulations (Y. Li et al., 2020; Ncubukezi, 2023; Udofot & Topchyan, 2020). By recognizing and addressing these interdependent elements, small retailers can improve their cybersecurity posture and reduce the risk of cyberattacks (Tam et al., 2021). The following section contains a discussion of employee training strategies in the prevention and management of cyberattacks on small retail businesses.

Employee Training Strategies

Training employees is an essential aspect of cybersecurity for modest retail businesses. To reduce the risk of cyberattacks, small retail business leaders should educate employees on how to identify and respond to prospective threats (Kusumastuti et al., 2020). However, employee training strategies are not devoid of difficulties and constraints. Training programs can effectively increase employees' awareness of cybersecurity threats and best practices by incorporating awareness and education components (Gulyas & Kiss, 2023). This knowledge enables them to recognize potential threats, such as phishing emails and suspicious websites, and prevent security intrusions by taking the necessary precautions.

By focusing on employee behavior, training strategies can resolve one of the greatest weaknesses of any organization: the human factor. By comprehending and applying cybersecurity best practices, employees can become the first line of defense against cyberattacks (Buresh & Esq, 2022). Small retail businesses leaders can tailor training programs to their particular requirements and priorities (Devi, 2023). This enables for more targeted training, ensuring that employees are aware of the specific threats and risks pertinent to their organization. Regular training updates and refreshers can help maintain a high level of cybersecurity awareness among employees (Y. Li et al., 2020). This continual education fosters a culture of vigilance, highlighting the significance of cybersecurity in daily operations.

While there are numerous strengths of current employee training programs, researchers have also highlighted numerous weaknesses. First, evidence suggests that small retail establishments often have limited budgets and resources for employee training (Kusumastuti et al., 2020). This limitation may result in fewer or lower-quality training programs, making it more difficult for employees to maintain their cybersecurity knowledge and skills. Additionally, developing and implementing effective training programs can be time-consuming, potentially distracting employees from their primary responsibilities (Franck & Reith, 2022). In small retail establishments where employees frequently wear multiple outfits, employee training programs can be a significant disadvantage.

Employees may resist alterations to their routines or behaviors, which makes implementing new cybersecurity practices difficult. Leaders of small businesses should combat this opposition by emphasizing the significance of security measures and offering incentives for compliance. Measuring the efficacy of employee training strategies can be challenging (Devi, 2023). Assessing the impact of training on employee behavior and the security posture of the organization as a whole can be difficult, making it difficult to determine whether training investments are profitable. Training programs may inadvertently contribute to overconfidence among employees, causing them to underestimate the likelihood or severity of cyberattacks (Y. Li et al., 2020). Small business leaders should strike a balance between employee confidence and a realistic understanding of the ever-changing threat landscape.

Employee training strategies can be an integral part of preventing and managing cyberattacks against small retail businesses. While there are numerous benefits to implementing training programs, small retail businesses leaders should also consider their limitations and difficulties (Y. Li et al., 2020). To optimize the effectiveness of employee training, small retail businesses should place an emphasis on customization, continuous learning, addressing resistance to change, and identifying methods for measuring the impact of training initiatives (Bahadoripour et al., 2023). The following section contains a presentation of evidence-based advice for professionals in similar positions based on what has been demonstrated in the current literature related to this topic.

Advice for Professionals in Similar Positions

Small retail business leaders need more IT skills and resources to adopt the latest cybersecurity advice. Many small retail business leaders need more security procedures to combat technologies' growing cyber threats and vulnerabilities (Jahankhani et al., 2022). Any company can suffer a loss of personal information or a data breach (Lloyd, 2020). Leaders of small retailers may have difficulty recovering from financial losses caused by cyberattacks (Chidukwani et al., 2022). A breakdown in trust, client loss, and decreased revenue are some adverse effects on small retail business leaders (Furnell et al., 2020). The general business problem under study in this research is that social media cyberattacks can negatively affect small retail businesses' viability and customer retention (R. Chen et al., 2021). The specific business problem is that some leaders of U.S. small business retailers lack strategies to deter social media cyberattacks.

Small retail business leaders should prioritize cybersecurity in order to safeguard their operations, consumer data, and reputation. Researchers recommend utilizing a risk-based strategy (Azubuike, 2021). Specifically, leaders can conduct regular risk assessments to identify and rank potential cyber threats and vulnerabilities. They should also prioritize addressing the most significant business hazards, according to the literature. Researchers also recommend creating a comprehensive cybersecurity policy outlining your organization's strategy for managing cyber risks, including roles and responsibilities, security measures, incident response procedures, and employee training (Devi, 2023). Effective cybersecurity protocols include all of these measures.

Researchers also advise providing employees with ongoing cybersecurity training and awareness programs. Business leaders should also educate them on best practices, common hazards like phishing and malware, and their role in protecting the data and systems of the organization. Researchers note that it is critical that small businesses maintain software and system updates (Franck & Reith, 2022). Software, operating systems, and firmware should be routinely updated on all devices, including point-of-sale systems, computers, and mobile devices. Outdated software may contain vulnerabilities that can be exploited by cybercriminals. Small retail business leaders should also utilize robust access controls (S. K. Khan et al., 2020). Business leaders should limit access to sensitive data and systems to only those employees who require it to perform their job duties, as well as use unique, strong passwords for every account, and enable multi-factor authentication (MFA) whenever possible.

Small retail business leaders should also implement encryption as part of their cybersecurity measures. Business leaders should protect sensitive data from unauthorized access by encrypting it both in transit and at rest (Y. Li et al., 2020). When transmitting data over the internet, business leaders should implement secure communication protocols such as HTTPS. Business leaders should also implement a firewall and use a Wi-Fi network with robust encryption to protect your network. Small retail business leaders should also monitor and update network security settings on a regular basis to protect against emerging threats. Researchers advise establishing a backup schedule for business-critical data and storing backups securely offshore or in the cloud (Devi, 2023; Gulyas & Kiss, 2023). Small retail business leaders should also implement backup and recovery procedures to ensure their efficacy in the event of a cyberattack.

Business leaders are advised to create a detailed incident response plan that outlines the steps to take in the event of a cyberattack, including how to identify, contain, eliminate, and recover from an incident, and regularly evaluate the plan’s efficacy by conducting employee training and simulations. Business leaders can improve their risk management skills by participating in industry groups or networks to share threat intelligence and best practices, and collaborate and share information (Devi, 2023; S. K. Khan et al., 2020; Tam et al., 2021). Collaboration can assist in enhancing an organization’s cybersecurity posture and keeping you abreast of emerging threats and trends.

Small retail businesses can benefit when leaders purchase cyber insurance. Business leaders can evaluate the advantages of purchasing cyber insurance to help mitigate the financial impact of a cyberattack (Azubuike, 2021). Cyber insurance can cover incident response expenses, legal fees, public relations expenses, and regulatory fines. It is also critical to review and update on a regular basis (Franck & Reith, 2022). Business leaders should review and update cybersecurity policies, procedures, and training on a regular basis to account for changes to business operations, emerging threats, and lessons learned from previous incidents or exercises (N. A. Khan et al., 2020). By following these measures, small retail business leaders can prevent and manage cyberattacks and cybersecurity threats more effectively, thereby protecting their operations, customers, and reputation. The following section contains a discussion of cyberattack planning.

Cyberattack Contingency Planning

Small retail business leaders should implement cyberattack contingency planning to mitigate the effects of cyber incidents, safeguard customer data, and ensure business continuity. A well-developed contingency plan outlines the steps to take prior to, during, and following a cyberattack (Kusumastuti et al., 2020). One way researchers have suggested to engage in this practice is to first conduct a thorough risk assessment to identify potential cyber threats and vulnerabilities unique to your organization (Devi, 2023; Y. Li et al., 2020). This method assists in prioritizing resources and concentrating on the most critical dangers (Y. Li et al., 2020). Additionally, small retail business leaders should assemble an incident response team with clearly defined roles and responsibilities (Tam et al., 2021). This committee should include members from departments such as IT, legal, human resources, and public relations. Organizational leaders should also ensure that all team members receive training on their respective roles and the incident response procedure as a whole.

Responding to cybersecurity incidents is an integral part of a company's cybersecurity protocols and measures. Researchers recommend that small business leaders develop a comprehensive incident response plan outlining the steps to be taken in the event of a cyberattack (Udofot & Topchyan, 2020). This strategy should include procedures for identifying and reporting security incidents, including containment strategies to limit the attack's effects and prevent additional damage, eradication and rehabilitation measures designed to eliminate the threat, restore systems, and resume normal operations, protocols for communicating the incident to employees, consumers, and relevant authorities, and post-incident analysis to identify lessons learned and implement preventative measures to avoid future incidents (Udofot & Topchyan, 2020). Small business leaders should also backup and have measures for the recovery of data. Researchers recommend that small business leaders implement a robust data backup strategy to ensure that vital business and consumer data can be recovered in the event of a cyberattack (Buresh & Esq, 2022). Regularly testing recovery procedures is also necessary to ensure their efficacy, and store backups securely off-site or in the cloud.

Cyber insurance is one mechanism small retail business leaders can use to mitigate the effects of cyberattacks. Researchers have suggested that small business leaders consider purchasing cyber insurance to reduce the financial impact of a cyberattack (Franck & Reith, 2022). Cyber insurance can cover incident response expenses, legal fees, public relations expenses, and regulatory fines. Employee training is also essential, and small business leaders should educate employees on best practices in cybersecurity and the procedures specified in your contingency plan (Gulyas & Kiss, 2023). Regular training can help ensure that employees are adequately prepared to respond to a cyberattack (Azubuike, 2021). The recommendation has also been proposed that small business leaders evaluate the cybersecurity posture of vendors and other third parties with access to systems or data. Small retail business leaders should also include provisions for incident response coordination in your contracts and establish clear expectations and prerequisites for their cybersecurity practices.

A complete cybersecurity plan includes having a contingency plan. Researchers also recommend that a review and updates be made to contingency plans on a regular basis (Y. Li et al., 2020). Small retail business leaders should review and update the contingency plan on a regular basis to account for alterations to your business operations, emerging cyber threats, and lessons learned from previous incidents or exercises. Leaders should consider conduct periodic exercises or simulations to evaluate your plan's efficacy and identify areas for improvement (Kusumastuti et al., 2020). Cyberattack contingency planning for small retail businesses entails a comprehensive strategy that addresses risk assessment, incident response, data backup and recovery, cyber insurance, employee training, third-party relationships, and routine plan reviews and updates (Puławska et al., 2022). By developing and maintaining a comprehensive contingency plan, small retail businesses can better secure their operations and customer data by preparing for, responding to, and recovering from cyberattacks. The following section contains a discussion of the application of this literature to the applied business problem underpinning this study.

Application to the Applied Business Problem

The purpose of this qualitative multiple-case study was to identify and explore strategies some U.S. retail leaders use to deter social media cyberattacks. By highlighting the many forms and implications of social media cyberattacks on companies, this study on cybersecurity supports the fact that some executives of U.S. small company retailers lack measures to counter these attacks. According to the literature, social media cyberattacks can take numerous forms, including phishing schemes, impersonation, and disinformation campaigns. They can have serious effects on businesses, such as loss of revenue, trust erosion, and theft of sensitive data.

GST also sheds light on the topic of social media cyberattacks and the necessity for preventive measures. GST presupposes that systems, including companies, are complex and linked and that changes in one element of the system might have unforeseen implications in other sections. GST implies that in the context of social media cyberattacks, these attacks can spread and inflict harm to a business's linked systems, such as its financial, reputational, and customer ties. As a result, small retail business leaders should have measures in place to discourage social media cyberattacks and secure their systems from harm.

Summary of the Literature Review

GST is an expansive framework for studying and understanding systems that may be applied to the study of cyber assaults to help uncover patterns and trends, as well as build tactics for detecting and mitigating these attacks. GST is made up of numerous critical components, including input, output, feedback, and homeostasis, all of which work together to keep a system stable and intact (von Bertalanffy, 1972). GST is used in the study of cyber assaults to examine connections and linkages between different aspects of a cyberattack system (Dias et al., 2022). This can aid academics and practitioners in identifying vulnerabilities and flaws in these systems, as well as developing tactics for detecting and preventing cyber assaults.

Preventing social media cyberattacks often entails a mix of technical and non-technical measures such as user education and awareness. Individuals and businesses should be updated about the current risks and take precautions to protect themselves and their networks. Due to limited resources and frequently lax security procedures, small retailers are particularly vulnerable to cyberattacks (Franck & Reith, 2022; Y. Li et al., 2020; Udofot & Topchyan, 2020). These attacks can result in severe financial losses, reputational harm, and lost customer trust for small retailers (Y. Li et al., 2020). Small stores should install robust security measures and train their personnel on cybersecurity best practices to prevent cyber assaults.

The research findings may be applied to the applicable business problem of cybersecurity threats by giving a framework for understanding and mitigating these attacks, as well as emphasizing the significance of adopting proactive actions to guard against these risks. The researcher's primary conclusions in this literature review include the necessity for small businesses to be vigilant and informed of the current threats and the need for continued efforts to avoid and mitigate cyberattacks.

Transition

Section 1 introduced the problem and purpose of this research. The population was described, and a target sample population was identified. The nature of the study was described in detail, followed by the research question, "What strategies do some leaders of small retail businesses use to deter social media cyberattacks?" The theoretical framework underpinning this study, GST, was introduced and later described in more detail as part of the introduction to the literature review.

Operational definitions are included in Section 1 to help orient the reader followed by the assumptions, limitations, and delimitations that frame this research. The significance of the study was provided and then a review of the literature followed.

The literature review included details on how the literature search was conducted and provided a detailed overview of GST as it is portrayed in the literature and applied to studies of a similar focus. A literature review on cybercrime, cyberattacks, and social media cyberattacks is provided and includes an overview of the literature that describes known prevention efforts. The following section provides insights into how small retail businesses are described in the literature in relation to small retailer cyberattack susceptibility, costs, and prevention efforts. Section 1 concludes with an overview of how the literature applies to the applied business problem and a literature review summary.

A description of the study's purpose, participants, research methods and design, population and sampling, ethical research, data collection instrument, data collection technique, data analysis, reliability, and validity is provided in Section 2. In Section 3, I will describe the findings of the study and how the findings apply to professional practice. Finally, Section 3 will conclude with implications for social change, recommendations for action, recommendations for further research, and any final reflections on the project.

Section 2: The Project

Cybercriminals are increasingly targeting small retail businesses using social media cyberattacks. On average, an employee of a small business with less than 100 employees will experience 350% more social engineering attacks than an employee of a larger enterprise (Raineri & Resig, 2020). In this study, I examined the strategies that small retail business leaders use to mitigate the adverse effects of social media cyberattacks.

Section 2 begins with a restatement of the purpose, my role as a researcher, and the details regarding my choice of a qualitative research methodology and multiple case study design. I also describe the participants, the sampling method and size, and the data collection instrument. I address the importance of adhering to the ethical guidelines prescribed by *The Belmont Report* and Walden University's Institutional Review Board (IRB). Section 2 also includes descriptions of the data collection, data organization, and data analysis procedures, as well as a discussion of strategies to ensure the reliability and validity of the study. A summary and transition to Section 3 is also provided.

Purpose Statement

The purpose of this qualitative multiple-case study was to identify and explore strategies some U.S. retail leaders use to deter social media cyberattacks. The target case population was 10 to 12 small retail business leaders in the United States who had successfully developed strategies and procedures to mitigate social media cyberattacks. Implications for positive social change include the identification of processes and risk management strategies small retail business leaders use to successfully mitigate and respond to social media cyberattacks.

Role of the Researcher

In qualitative studies, the role of the researcher is multifaceted. According to Fusch et al. (2018), qualitative researchers are responsible for selecting participants and organizing and analyzing data. The researcher is primarily responsible for collecting all data used in the study, including interviews, observations, artifact or document reviews and the researcher's reflections (Merriam & Grenier, 2019). Yin (2018) identified the following seven roles of a researcher undertaking a qualitative study: (a) data collection, (b) data organization, (c) data analysis, (d) data interpretation, (e) reviewing the academic literature to gather background information relevant to the research problem, (f) identification, recruitment and engagement of the participants, and (g) data storage and security. In this qualitative case study, I served as the primary research instrument.

One of my roles as a researcher was to collect and analyze data on the strategies that small retail business leaders use to mitigate and respond to social media cyberattacks. Other roles include recruiting and conducting interviews with small retail business leaders, audio-recording the data provided by the participants in virtual semistructured interviews, transcribing the audio recordings, and coding and organizing the data into themes. In this study, I accessed the participants using an informed consent form, a participant invitation email, and an interview protocol (see Appendix).

Researchers must also adhere to the ethical principles and guidelines outlined in *The Belmont Report* for protecting human research subjects from abuse or harm (National

Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). *The Belmont Report* aims to ensure that researchers adhere to three principles: (a) respect for persons, (b) beneficence, and (c) justice (Paxton, 2020). I adhered to these three principles by allowing the participants to assess the risks and benefits of participating in the study and voluntarily joining the study through informed consent.

My role as a qualitative researcher included protecting the study participants' ethical and moral rights. I ensured adherence to *The Belmont Report* using the following measures. First, I communicated with the participants regarding the purpose of the research study and explicitly delineated the research procedure. Second, I informed the participants about the risks and benefits associated with participation in the study. Third, I completed Collaboration Institutional Training Initiative (CITI) training course on protecting human research participants. Finally, I complied with the Walden University research protocols and follow the regulations of the IRB. I used these measures to ensure that I complied with the guidelines of *The Belmont Report*.

Qualitative researchers must also follow measures to mitigate research bias. I used various reflexivity protocols to mitigate researcher bias (see Yin, 2018). First, I ensured that participants voluntarily participate in the study using the informed consent form. Second, I used an interview protocol to ensure all participants were asked the same questions. Third, I used interviewee transcript review (see Rowlands, 2021) and member-checking of the data (see Candela, 2019) to ensure validity. Fourth, I used journaling and memoing to ensure that my perceptions as a researcher were thoroughly documented throughout the research process (see McGrath et al., 2021). I used these mechanisms to mitigate the potential limitations of researcher bias.

Participants

I recruited participants in several phases. In Phase A, I leveraged my professional network and request that my network disseminate the recruitment flier to individuals who were leaders of small retail businesses in the United States. To maintain a rigorous level of objectivity, I excluded individuals with whom I had direct prior professional interactions. In Phase B, I used social media aimed at supporting small retail business leaders to recruit participants for this study. I obtained the permission of group moderators, who were asked to post the recruitment flier on the group's platform. For this qualitative multiple case study, the eligibility criteria for participation were that individuals must (a) be over 18 years of age, (b) be the leader of a small retail business in the United States, (c) use social media to conduct part or all of their retail business, and (d) have demonstrated success in mitigating cyberattacks. Qualitative research is based on the premise that the participants have in-depth knowledge about the phenomenon under investigation (Yin, 2018). The small retail business leaders in this target group were suitable for this research study because they have direct knowledge of the business strategies used to mitigate social media cyberattacks in their firms.

I used purposeful sampling to determine the participants in this study. Purposeful sampling is a sampling method used by researchers to select participants with intricate knowledge of the phenomenon under investigation (Staller, 2021). Purposeful sampling is a technique in which information-rich cases are chosen based on a set of qualifying criteria (Staller, 2021). A benefit of purposeful sampling in qualitative research includes obtaining valuable information from the participants with limited research resources (S. Campbell et al., 2020). Purposeful sampling also mitigates some aspects of sampling bias associated with convenience, quota, or stratified sampling (Baltes & Ralph, 2022). I used the purposeful sampling technique to select small retail business leaders with extensive knowledge of successful strategies for mitigating social media cyberattacks.

Research Method and Design

There are three main research methods: qualitative, quantitative, and mixed methods. Researchers use the qualitative method to explore why and how people behave and interact in social and professional settings (Busetto et al., 2020). I used the qualitative method to investigate the strategies small retail business leaders use to prevent and mitigate social media cyberattacks. Within the qualitative tradition, researchers can choose between various research designs, including case studies, phenomenological, ethnographic, and narrative inquiry (Denzin & Lincoln, 2018). Researchers should choose a research design that aligns with the research method to answer the central research question of the study (Yin, 2018). In this study, I selected the multiple case study design.

Research Method

I chose the qualitative method in this study to explore the strategies small retail business leaders use to prevent and mitigate social media cyberattacks. A quantitative researcher gains insight into the phenomenon under investigation through inductive examination of the study participants' perceptions, experiences, and beliefs (Prosek &

Gibson, 2021). Qualitative methods are also appropriate for examining how a particular population interacts with others in meaningful ways (Allan, 2020). The qualitative methodology was appropriate for this study because I wished to explore the strategies used by small retail business leaders to mitigate social media cyberattacks and the participants' perceptions of the efficacy of those strategies.

Quantitative researchers use statistical data to evaluate cause-and-effect relationships between numerical variables. The quantitative methodology is appropriate for research questions investigating the frequency or statistical nature of an event or testing hypotheses regarding correlations and relationships between variables (Mohajan, 2020). The quantitative method was, therefore, not appropriate for this study investigating the behaviors of small retail business leaders in response to social media cyberattacks. Mixed methodology, which combines aspects of quantitative and qualitative studies, was also not appropriate for this study. Researchers use mixed methods to answer research questions that cannot fully be evaluated using qualitative or quantitative methods alone (Dawadi et al., 2021). I ruled out the use of mixed methodology because the study's research question lacks a quantitative component. Therefore, a qualitative research method was most appropriate for this study.

Research Design

There are five main types of qualitative research designs: case study, phenomenological, ethnography, narrative inquiry, and descriptive (Busetto et al., 2020). I used a multiple case study design for this study. The case study design was appropriate to explore the strategies that small retail business leaders use to prevent, deter, and mitigate social media cyberattacks. Researchers using the qualitative case study design collect in-depth data from multiple sources to allow for data triangulation (Kekeya, 2021), which enhances the reliability and validity of the study (Quintão et al., 2020). The choice of a qualitative case study design allows researchers to examine questions related to how and why a particular phenomenon occurs in a given context and when interventions into the participants' behavior are not appropriate or desired (Kekeya, 2021). The aim of this study was to examine how small retail business leaders mitigate and deter social media cyberattacks, a purpose consistent with a case study design.

There are two types of case study designs: single and multiple. Researchers use a single case study design when they seek to understand the intricacies regarding a single case with respect to a particular phenomenon (Kazdin, 2021). For example, a single case study design would be appropriate for an exploration of the perceptions of different stakeholders, namely managers, employees, and administrators, within the same retail company regarding social media cyberattacks. A researcher uses the multiple case study design to investigate a particular phenomenon across multiple cases and settings (Farquhar et al., 2020). I chose a multiple case study research design because it was an appropriate design for gaining the perspectives of multiple small retail business leaders regarding effective strategies for deterring social media cyberattacks.

I ruled out phenomenological, ethnographic, and narrative inquiry research designs. Phenomenology is appropriate research design for researchers seeking to understand the lived experiences of individuals (Hourigan & Edgar, 2020). I did not choose a phenomenological research design because the purpose of this study was to examine effective strategies for deterring social media cyberattacks, not to explore the lived experiences of small retail business leaders. The ethnographic research design is used to study a population's culture, behaviors, and social interactions over an extended period of time (Wutich & Brewis, 2019). The aim of the present study was not to examine the culture, behavior, and social interactions of small retail business leaders, but rather to understand strategies they employ to mitigate social media cyberattacks. An ethnographic research design was, therefore, not appropriate for this study. Researchers use narrative inquiry research designs to experience and retell the events experienced by participants through their life stories. I did not choose a narrative research design because it was not appropriate to answer the question of effective strategies small retail business leaders use to deter social media cyberattacks.

Population and Sampling

The general population of this study was small retail business leaders in the United States. The target population was small retail business leaders in the United States who successfully employed strategies to deter social media cyberattacks. The sample consisted of 11 purposefully sampled small retail business leaders in the United States who successfully employed strategies to deter or prevent social media cyberattacks. The participants met the following inclusion criteria: (a) over 18 years of age, (b) the leader of a small retail business in the United States, (c) uses social media to conduct part or all of their retail business, and (d) has demonstrated success in mitigating cyberattacks.

Using an appropriate sampling technique is critical for qualitative studies. In qualitative research, researchers can choose between convenience, purposeful, and snowball sampling (Yin, 2018). Convenience sampling is a method used to conveniently select participants based on ease of access, budget, or proximity to the researcher (Stratton, 2021). Purposeful sampling is a technique in which information-rich cases are chosen based on a set of qualifying criteria (Staller, 2021). Snowball sampling relies on current study participants referring or nominating other individuals who meet the study's inclusion criteria (Parker et al., 2019). I used purposeful sampling to identify participants who are knowledgeable about the phenomenon of strategies to deter and prevent social media cyberattacks because this sampling technique allowed for the identification of participants with sufficient knowledge to answer the study's research question (see Stratton, 2021).

The recruitment flier contained a QR code with a link to a participant screening questionnaire that assessed a potential participant's eligibility for inclusion in the study. The questions on the screening questionnaire were the following:

1. What is your age?
2. Are you the leader of a small retail business in the United States? [Yes/No]
3. Do you use social media to conduct part or all of your retail business? [Yes/No]
4. Have you demonstrated success in mitigating social media cyberattacks? [Yes/No]

I evaluated potential participants' candidacy for inclusion in the study using the participant screening questionnaire. For inclusion in the study, participants needed to answer Question 1 with an answer of "over 18 years old" and must have answered "yes" to Questions 2, 3 and 4. Any other combination of answers disqualified the potential participant from inclusion in the study.

Data saturation influences the strengths of the conclusions that researchers can draw in qualitative research. Data saturation is defined as the point in data collection at which interviewing more participants would not result in the identification of new themes (Braun & Clarke, 2021). Guest et al. (2020) found that in 98% of interview-based qualitative students, data saturation was reached after eight participant interviews. A sample size of 11 participants was sufficient to reach data saturation. Data saturation is evidenced by the repetition of themes and ideas by the participants (Low, 2019). In this study, data saturation was evidenced by no new codes being derived from the interviews of participants P10 and P11.

Ethical Research

I followed stringent ethical guidelines during this research study. The research was limited to work-related interviews, which posed minimal risk to the participants, and no sensitive or emotional topics were explored. I submitted the study for approval through the Walden University IRB application process and only commenced the study once authorization and approval had been granted (IRB Approval #06-21-23-0399485). The well-being of the participants was maintained throughout the study by adhering to established ethical norms, as stated in *The Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). To this end, I upheld the principles of justice, kindness, and respect for people throughout the study.

I used informed consent forms to ensure that each participant willingly and voluntarily agreed to participate in the research. After potential participants identified their interest in the study by filling in the participant screening questionnaire, I emailed them the participant invitation letter that included an informed consent form. The informed consent form addressed important ethical issues, including the study's risks and advantages, the participant's right to withdraw from the study at any time and the procedures I used to ensure their confidentiality and anonymity. Specifically, to safeguard the participants' confidentiality and privacy, I communicated with the participants through secure methods and did not post any questions on public forums. I ensured that the participants knew that they could withdraw from the study at any time without fear of repercussion. No participants decided to withdraw from the study. However, if a participant had decided to withdraw from the study, I would have destroyed all data collected from the participant, except for their informed consent form and documentation of their withdrawal. There were no incentives given to participants for participation in the study.

I coded all participant-derived data files, including informed consent forms, screening questionnaires, audio recording files and interview transcripts with participant numbers (P1, P2, etc.). If a participant mentioned information that could have reasonably identify them, including their place of employment, that information was redacted from their interview transcript to protect their confidentiality. In addition, I removed all personally identifiable information, including participants' names and places of employment, from the interview transcripts. As mandated by Walden University, I safely archived the raw data, including recordings and transcripts, and analytical data for 5 years. I also safely stored the informed consent forms for 5 years, as required by the Walden University IRB. I stored all research-related materials and data on a password-protected, encrypted cloud drive. After 5 years, I will destroy the data using data destruction software.

Data Collection Instruments

There were two instruments in this multiple case study. The researcher was the first instrument, as described in the role of the researcher subsection. The second instrument was an interview guide consisting of open-ended interview questions that served as the qualitative tool for data collection (see Appendix). I developed the interview guide based on the study's purpose, research question and theoretical foundation. The interviews focused on key inquiries about the participants' perspectives on social media cyberattacks and the strategies they used to deter and mitigate such attacks. The open-ended interview questions allowed for a systematic and methodical exploration of the participants' experiences and insights. I enhanced the reliability and validity of the data collection process through interviewee transcript review (see Rowlands, 2021) and member checking (see Candela, 2019).

The interview protocol was validated using two mechanisms. First, I used peer review by other Walden University students with expertise in business and cybersecurity. I considered and incorporated appropriate feedback from peer review into the interview protocol. Second, I submitted the interview protocol to my dissertation committee for expert panel review. I incorporated all changes and feedback into the interview protocol prior to submission to the Walden University IRB for approval. These procedures ensured that the interview protocol addresses the research questions within the chosen theoretical framework for the study.

Data Collection Technique

In this subsection, I discuss the following procedures regarding data collection: (a) participant screening and informed consent procedures, (b) procedures for participation, and (c) data collection procedures. Data collection will proceed using semistructured interviews with participants meeting the study's inclusion criteria. I discuss the advantages and disadvantages of using semistructured interviews for data collection in the Procedures for Participation section. Procedures employed to enhance the reliability and validity of the study, including interviewee transcript review and member checking, are described in the Data Collection Procedures section.

Participant Screening and Informed Consent Procedures

The participants were recruited as described in the Participants subsection. Participants interested in participating in the study were instructed by the recruitment flier to scan a QR code containing a link to a participant screening questionnaire. After participants filled in the questionnaire, I notified them by email of their inclusion or exclusion from the study. Participants who met the inclusion criteria were invited to participate in the study when I sent them the participant invitation email. I also included an informed consent form in the participant invitation email. Participants were instructed to read the informed consent form and reply to the email with the words "I consent." The informed consent form explained the study’s voluntary nature and the participants’ freedom to discontinue participation at any time.

Procedures for Participation

Once participants completed and submitted the informed consent form, I sent them a link to my Calendly, an online scheduling application, to choose a time and date to participate in the semistructured interviews. At each participant’s selected time and date, one-on-one interviews were conducted via Zoom telecommunications software, as this platform provided a safe research environment. The interview method was suitable for the study, as the method enabled direct engagement with small retail business leaders in the United States with experience in mitigating and deterring social media cyberattacks. I was responsible for following the interview guide (see Appendix), posing open-ended questions, facilitating the interview sessions, and ensuring data clarity in communication. Each participant participated in one interview lasting between 30 and 45 minutes, giving each participant time to expand on their points of view.

Semistructured interviews have several advantages and are an effective data collection tool for qualitative research studies. Interviews can proceed according to multiple modalities, including in-person, virtual, or written interviews. I chose to use virtual semistructured interviews using the Zoom telecommunications software because this modality offers researchers the flexibility to expand on participants’ responses while observing valuable information from verbal and non-verbal behaviors (see Yin, 2018). Semistructured interviews allow researchers to ask clarifying or probing questions to gain further insight into their primary responses (Brown & Danaher, 2019). For this study, I followed the interview protocol, which contained open-ended questions (see Appendix), and asked probing questions when I needed clarification on a participant's response.

Semistructured interviews have some disadvantages. For example, these types of interviews take considerable time and require the researcher to have multiple exchanges with participants to schedule and complete the interviews (Yin, 2018). Interviews that take place virtually, such as the ones in this study, could also be impacted by technological or connectivity considerations. Data could be lost if there's a failure of the software used to record or conduct the interview. This limitation can be mitigated if the researcher tests the interview platform and recording equipment. I conducted a pilot test of the semistructured interview protocol with a colleague who provided reasonable answers to the questions. This allowed me to test the interview and recording platforms and practice.

Data Collection Procedures

On the day of each scheduled interview, I kept an audio trail of the interviews, with the explicit permission of the participants. Keeping an audio trail allowed me to ensure that the audio was transcribed accurately (Yin, 2018). I aimed to obtain a rich and thick set of data from the participants, which reduces researcher and participant bias while improving data saturation (Johnson et al., 2020). To ensure a thick description, I asked probing questions and requested clarification on incomplete or partial answers. After the interviews were complete, I transcribed the interviews. First, I Otter.ai's automatic transcription tool. Second, I compared the interview transcripts line-by-line with the audio recording to ensure the accuracy of the transcripts. Any personally identifiable information revealed by the participants, such as their names or places of employment, was redacted to preserve the participants' confidentiality.

I used interviewee transcript review and member checking to enhance the validity and reliability of the study's findings. After transcription, I sent the transcripts to the participants for interviewee transcript review. Interviewee transcript review is a quality control mechanism that researchers can use to enhance the credibility of the research findings (Rowlands, 2021). During this process, I provided the participants with a copy of the transcript to allow them to confirm that their answers accurately reflect their ideas. Five participants (P3, P5, P8, P9, and P11) responded to the interviewee transcript review, indicating that no changes to the transcripts were required. I also review company records for data triangulation to help increase the trustworthiness of the study. Specifically, the participants provided me with documents regarding their cybersecurity software purchases, including anti-virus and malware software. Finally, I used member checking after the data interpretation was complete. Member checking is another quality control mechanism researchers use to enhance the credibility of their qualitative studies (Candela, 2019). During member checking, I emailed each participant a one-page summary of their analyzed data to ensure my interpretation of their responses was consistent with their thoughts and ideas. Four participants (P1, P3, P9, and P10) responded to the member checking email, indicating they agreed with my interpretation of their data.

Data Organization Technique

I used a research log to note the explicit details regarding the procedures I used to conduct the research study. During the study, I coded each participant’s interview transcripts and question responses using a unique alphanumeric identifier, such as P1, P2, P3, … and P11, to ensure participant confidentiality. I organized the data using NVivo Version 12, a qualitative data analysis software that has proven use in managing and storing research data (see Alam, 2021). The NVivo program also allowed me to keep an accurate record of the research process by allowing me to make reflexive memos and keep a reflexive journal. In my reflexive journal, I made notes regarding my perceptions of the participants’ responses and behaviors. Journaling and memoing are important mechanisms that researchers can use to ensure their own reflexivity and mitigate researcher bias (McGrath et al., 2021). I stored all electronic data collected during my study on a secure, password-protected, encrypted cloud drive. After 5 years has elapsed, I will use data destruction software to destroy all electronic data, as mandated by the Walden University IRB.

Data Analysis

Qualitative researchers are responsible for conducting data analysis to present valid and reliable findings, while enhancing the trustworthiness of the study. According to Kiger and Varpio (2020) There are five main types of theme-based data analysis: (a) comparative analysis, (b) content analysis, (c) cross-case synthesis, (d) narrative synthesis, and (e) thematic analysis. I used Braun and Clarke’s (2019) method for thematic analysis, employing the NVivo (Version 12) software for data compilation, sorting, and coding (see Alam, 2021). After data analysis was complete, I sent participants a one- to two-page summary of the findings for member checking as a mechanism to enhance the reliability and validity of the study's findings (see Candela, 2019).

Triangulation is an important data analysis technique used in qualitative studies. The multiple case study research design relies on the convergence of multiple data sources, such as interview data and supplementary documentation, to enhance the validity and reliability of the research study (Yin, 2018). Triangulation is an important aspect of qualitative data analysis. Triangulation involves comparing information from multiple sources to determine if the information corroborates each other (R. Campbell et al., 2020). Researchers use triangulation in qualitative research to minimize researcher bias, provide richness to the data collection, and aid in reaching data saturation (R. Campbell et al., 2020). There are four types of triangulation. Data triangulation involves the use of multiple sources of data; investigator triangulation involves using multiple researchers to conduct the study (Natow, 2020). Theory triangulation involves analyzing the same data set from the vantage of multiple theoretical frameworks; methodological triangulation involves the use of multiple research methods (Natow, 2020). In this study, I used data triangulation by evaluating data from multiple sources, including participant interviews and company documents provided by the participants.

Triangulation is an important component of qualitative research studies. Natow (2020) describes the use of triangulation of multiple sources, researchers, methods, and frameworks to identify and eliminate alternative explanations for the findings in qualitative research studies. Researchers use triangulation to mitigate researcher bias and aid in achieving data saturation (Yin, 2018). There are other mechanisms researchers can use to reduce researcher bias, including using an interview protocol, conducting interviewee transcript review (Rowlands, 2021) and member-checking (Candela, 2019), and reflexivity protocols (McGrath et al., 2021). I used each of these steps to help reduce researcher bias.

I analyzed the data collected from semistructured interviews through thematic analysis. Thematic analysis is a common approach used to analyze large amounts of verbal data (Lindgren et al., 2020). As Raskind et al. (2019) described, the data analysis process involves organizing and dissecting the data to identify themes and patterns relevant to the research questions, enabling the researcher to make inferences. Specifically, I analyzed the interview transcripts using Braun and Clarke's (2019) method for thematic analysis, a six-phase guide, including familiarizing with the interview data, categorizing data and developing codes, reviewing and extracting themes, creating a thematic map, continuously defining and refining themes, and analyzing the themes and subthemes gathered from the interviews. Thematic analysis is a widely used qualitative research method for analyzing data collected from semistructured focus groups, interviews, and other qualitative data sources (Braun & Clarke, 2019). Data analysis is a methodical and systematic process that allows researchers to extract meaningful themes and patterns from the collected data (Braun & Clarke, 2019). Each phase will be discussed in turn.

Phase 1: Familiarization With Data

In this phase, I became familiar with the interview data by transcribing the audio files into transcripts. I read each interview from start to finish to get an overall understanding of the data collected. This phase often involves multiple readings of the interview transcripts. Specifically, after reading each participant's interview transcript from start to finish, I read each interview according to the interview questions across participants. During this phase, I ensured that the participants' personally identifiable information in the interview transcripts was redacted.

Phase 2: Coding

Phase 2 was the coding phase. This phase involved categorizing the data into meaningful units, also known as coding (Saldaña, 2021). During this phase, I created a codebook that outlines the codes for categorizing the data. The codes were applied to the data to identify the participants' ideas, thoughts and opinions. I used a combination of a priori and emergent coding, following Saldaña (2021). A priori codes were developed based on the study's theoretical framework, GST.

Phase 3: Theme Development

During this phase, I reviewed the coded data and extracted themes from the codes. The themes represent patterns and relationships between the data (Braun & Clarke, 2019). To this end, I grouped similar codes categories. Categories where then analyzed and grouped into themes.

Phase 4: Thematic Map

In this phase, I created a thematic map that revealed the connections between the codes and themes. The map helps researchers organize the data analysis logically and coherently (Braun & Clarke, 2019). This approach allowed me to identify the congruency of themes and the differences between themes.

Phase 5: Refining Themes

During Phase 5, I examined the thematic map and evaluate whether any new themes have emerged. If necessary, I renamed and redefined the codes and themes to guarantee the veracity and completeness of the analysis. Specifically, I redefined and reclassified similar themes into a new overarching theme to remove redundant themes. I addressed discrepant cases in this phase. There were no discrepant cases identified by the data analysis.

Phase 6: Data Analysis and Interpretation

In this final phase, I looked holistically at the data and data analysis to ensure that each research topic had a logical meaning. During this phase, I ensure that the research question had been answered thoroughly through the data analysis. I also interpreted the data in the context of the study's theoretical framework. Finally, after data analysis and interpretation were complete, I summarized each participant's data and performed member checking (see Candela, 2019). These steps enhanced the credibility and validity of the study's findings.

Reliability and Validity

In qualitative studies, it is essential to consider the suitability of instruments, procedures, and data to ensure that the research findings are both valid and reliable. Lemon and Hayes (2020) define the trustworthiness of a study as the level to which a researcher has confidence in the quality of the data, the transcriptions, and the procedures used to collect and analyze the data. Reliability and validity are terms used to describe the rigor of quantitative studies (Lemon & Hayes, 2020). The corresponding ideas for qualitative research are dependability, confirmability, transferability, and credibility (Stahl & King, 2020). I will discuss dependability in the context of reliability and confirmability, transferability, and credibility in the context of validity.

Reliability

Reliability is an essential component of all research studies. In qualitative research, reliability refers to the soundness of the research pertaining to the methodology, research design, sampling method, and ways in which the data are analyzed (Vu, 2021). There are several strategies researchers can employ to improve the reliability, or dependability, of qualitative research, including: (a) identifing researcher biases, (b) reporting any preconceived assumptions or notions, (c) be ingrigorous in establishing the participants and methods, and (d) accurately reporting the information provided by the participants (Rose & Johnson, 2020). I used various methods, including extensive researcher reflexivity protocols, to enhance the reliability and dependability of the study, as described in the next section.

Dependability

Dependability is a method of establishing rigor and trustworthiness in qualitative studies that relies on the use of rigorous protocols for data collection and analysis. In this study, I ensured the dependability of my findings in the following ways. First, I documented my research protocol in my research log to provide rigor in the establishment of the participants and research methods. Second, I kept a reflexivity journal to note any preconceived notions, thoughts, and perceptions at each stage of the research process, following the guidance of McGrath et al. (2021). Third, I employed interviewee transcript review (see Rowlands, 2021) and member checking (see Candela, 2019) to allow the participants to review the transcripts and data summary for errors and confirm my data interpretation. These methodological choices enhanced the dependability of the study's findings.

Validity

Qualitative researchers achieve validity, or credibility, using multiple sources of evidence and establishing a chain of evidence. Rose and Johnson (2020) noted that qualitative researchers improve the validity of their findings through data triangulation and data saturation. According to Halkias et al. (2022), qualitative studies achieve external validity, or transferability, by evaluating multiple cases, triangulating findings, and comparing findings to those in the academic literature. Validity of a qualitative study is assessed through credibility, transferability and confirmability.

Credibility

Credibility refers to the believability of a research study. According to Wood et al. (2020), credibility involves the level of confidence that readers can have in the conclusions of the study. I ensured credibility in multiple ways. First, I used multiple data sources, combining data from the interview findings and documentary evidence from public records. This will allow me to provide a rich, thick data description and ensure data saturation (Rose & Johnson, 2020). I also kept a reflexive journal throughout the research process to document my perceptions of the research process, following the guidelines of McGrath et al. (2021). I also used member checking to ensure the accuracy of the information presented in the research findings.

Transferability

Transferability is similar to the concept of generalizability in quantitative studies. Specifically, transferability refers to the ability to generalize the research findings to other cases with similar individuals (Rose & Johnson, 2020). Transferability also refers to the extent to which other researchers can use and apply the study results beyond the boundaries of the initial population under investigation (Halkias et al., 2022). To address transferability, I documented my data collection and analysis methods rigorous, provide a detailed description of the interview protocol, case study, participants and research findings. According to S. Campbell et al. (2020), the purposeful sampling technique can also enhance the transferability of a study’s findings. I addressed transferability by ensuring that the purposefully selected participants interviewed in the study are diverse and representative of the study’s general population.

Confirmability

Confirmability refers to the extent to which the research findings can be replicated by other researchers. The confirmability of a study can be enhanced by rigorously documenting the study's anticipated and actual methodology (Halkias et al., 2022). To achieve confirmability in my study, I used an interview protocol for the semistructured interviews. I accurately documented the interview transcripts and performed member checking to verify the veracity of the data collected and its interpretation (see Candela, 2019). To minimize researcher bias, I used reflexivity protocols, including journaling and memoing to document my perceptions as a researcher.

Data saturation is important for confirmability. Data saturation is the point at which no new information will be gained by interviewing more participants (S. Campbell et al., 2020). Once saturation has been reached, data collection is thought to be exhausted (S. Campbell et al., 2020). To achieve data saturation, I interviewed as many small retail business leaders as needed until no new data or coding emerged. In this study, data saturation was evidenced by the number of unique codes generated by the participants, as shown in Table 1.

Table 1

Unique Codes Generated by the Participants' Interviews

Participant	Interview length	Number of unique codes
P1	30:14	21
P2	30:25	8
P3	21:34	2
P4	18:33	4
P5	26:13	1
P6	15:17	0
P7	13:35	0
P8	18:25	0
P9	18:10	1
P10	17:39	0
P11	19:49	0

As shown in Table 1, five of the eleven interviews did not generate any new codes during data analysis, indicating data saturation had been reached. In addition, I used multiple sources, including company documents regarding cybersecurity, and different cases to gather diverse information until the study reached saturation

Transition and Summary

In Section 2, I restated the purpose of the study and discussed my role as a researcher. I reported the participant selection criteria, recruitment strategy, research methodology and design. I identified the population, sample, sampling technique and discussed ethical research principles applicable to this study. I described procedures for participation, data collection, and data analysis. I also discussed the procedures I used to ensure the reliability and validity of the study. In Section 3, I will present the research findings, applications for professional practice and recommendation for future research.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple-case study was to identify and explore strategies some U.S. retail leaders use to deter social media cyberattacks. The theoretical framework was GST. Eleven U.S. small retail business leaders who successfully mitigated social media cyberattacks were interviewed in this study. The participants provided the primary data used to answer the research question, and secondary data sources included company documents regarding cybersecurity. Interviews were performed until data saturation was reached, as evidenced by the generation of no new information from the interviews or document review.

The participants discussed strategies they used to successfully mitigate social media cyberattacks. Based on the participants' responses to the interview questions, I identified three themes. The first theme is that U.S. small retail business owners employ multiple strategies to prevent social media cyberattacks. Second, the participants emphasized the education of employees and customers for mitigating social media cyberattacks. Finally, the third theme was that a contingency plan is necessary in the case of a social media cyberattack. By relating the study's findings to GST, I better understood some U.S. small retail business leaders' strategies to prevent social media cyberattacks. The study findings illustrate that some U.S. small retail business leaders use various mitigation strategies for social media cyberattacks.

Presentation of the Findings

The overarching research question guiding this study was: What strategies do some leaders of U. S. small retail businesses use to deter social media cyberattacks? Social media can be a powerful tool for marketing, customer management, and customer retention (Wibowo et al., 2020). However, the use of social media can also increase vulnerability to cyberattacks (Humayun et al., 2020). The literature suggests that small retail businesses are more vulnerable to cyberattacks than larger enterprises because fewer resources are available to combat them (Chidukwani et al., 2022). Small retail business leaders without effective cybersecurity measures could lose profitability after a social media cyberattack. I used triangulation to combine the data collected from semistructured interviews and company documents. Upon completing my sixth interview, no new codes were generated, indicating that I had reached data saturation. The number of unique codes generated by the participants' interviews is shown in Table 1 in Section 2. An additional five interviews were completed to ensure saturation had been reached.

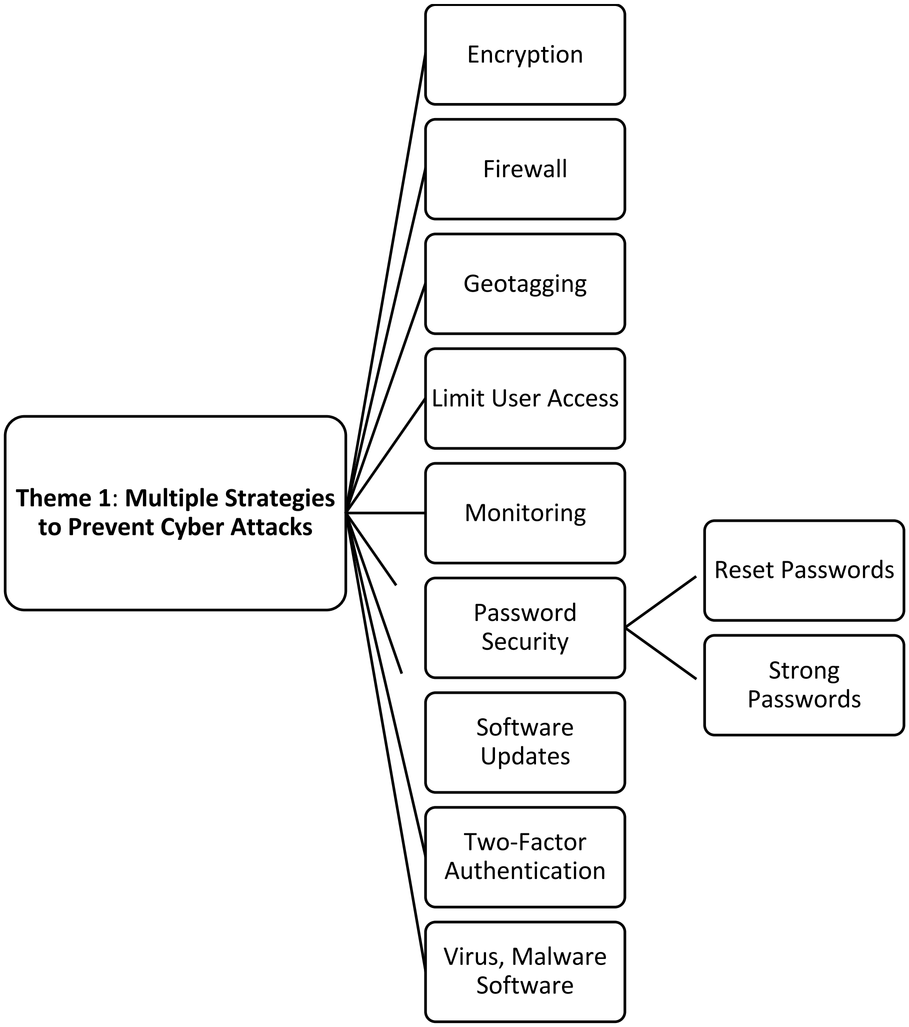
I organized the study data and conducted the thematic analysis using NVivo (Version 12) software to identify emerging themes and trends for data analysis and interpretation. Three themes were identified based on the participants' responses to the interview questions. The first theme is that U.S. small retail business owners employ multiple strategies to prevent social media cyberattacks. The second theme was an employee and customer education to mitigate social media cyberattacks. The third theme was that a contingency plan is necessary when encountering a social media cyberattack.

Theme 1: Multiple Strategies Are Used to Prevent Social Media Cyberattacks

The small retail business owners interviewed in this study described using multiple strategies for preventing social media cyberattacks. This theme directly answers the study's research question: What strategies do some leaders of U. S. small retail businesses use to deter social media cyberattacks? The codes that contributed to this theme are shown in Figure 1.

Figure 1

Codes Used to Develop Theme 1



The participants discussed eleven strategies for preventing social media cyberattacks. These strategies are described in Table 2. A description of each strategy as indicated by the literature is provided.

Table 2

The Participants Used Multiple Prevention and Mitigation Strategies

Strategy	Description	Participants
Encryption	Encryption is a way of protecting data by scrambling data requiring a unique key to unlock data (Madhuri & Prabhu, 2023).	P2, P4, P5, P7
Firewall	A firewall is a network security device that monitors traffic to or from a network. It allows or blocks traffic based on a defined set of security rules (Kim et al., 2020).	P1, P2, P3, P5, P7, P9, P10
Geotagging	Geotagging is the process of assigning geographic coordinates to media based on the location of the originating device (Khatoon et al., 2022).	P2, P5
Limit user access	Limiting employee access to consumer credit card information can mitigate social media cyberattacks (Salahdine & Kaabouch, 2019).	P1, P2, P4, P6, P9
Monitoring	Monitoring systems and users can help mitigate social media cyberattacks (Salahdine & Kaabouch, 2019).	P1, P2, P5, P6, P7, P9, P10, P11
Reset passwords	Cybersecurity experts suggest resetting passwords every 30 days (Pearman et al., 2019).	P2, P5, P8, P10
Separate personal and business affairs	Cybersecurity experts suggest that employees don’t use their personal devices to conduct business (Furnell & Shah, 2020).	P4, P10
Software updates	Outdated software can lead to system vulnerabilities for social media cyberattacks (Chigada & Madzinga, 2021).	P1, P3, P4, P5, P7, P8, P9, P10
Strong passwords	Strong passwords are unique alphanumeric combinations without reference to personal details (Dupuis et al., 2021).	P1, P2, P5, P7, P8, P9, P10, P11
Two-factor authentication	Two-factor authentication is when a user is granted access to a website or application only after they present two pieces of evidence to an authentication mechanism (ALSaleem & Alshoshan, 2021).	P2, P3, P8, P9, P10
Virus, malware software	Outdated virus and malware software can lead to system vulnerabilities for social media cyberattacks (Chigada & Madzinga, 2021).	P1, P2, P3, P5, P6, P9, P10, P11

The multifaceted nature of the participants' prevention and mitigation strategies that the problem of understanding strategies to mitigate social media cyberattacks is well suited for analysis under GST, the study's chosen theoretical framework. Each strategy elucidates by participants is now discussed.

Encryption

Encryption was the first strategy used by participants to deter social media cyberattacks. Encryption is the process of protecting data or information by scrambling it using mathematical means (Kamal et al., 2021). Four participants (P2, P4, P5, and P7) mentioned the importance of using encryption. For instance, P4 said,

> If you go with one of the largest credit processing companies in the nation at the absolute top-tier premium, they give me an encrypted, I want to call it almost like a token, but it's an encrypted device that the card has to be present, it's run through it has multiple layers of encryption.

P4 described using encryption to protect his consumer's credit card and financial data, a service provided through partnerships with credit card companies. P7 also described using encryption to protect customer information. P7 explained,

> We use a couple of different methods, one primarily being encrypted connections for customer data transmission. If you're going to be transferring information from one device to the other, you just don't want to do it on the open network. You want to have it on a secure network, so you can't have a man-in-the-middle attack on it.

P7 explained that encryption can protect customer data and prevent man-in-the-middle attacks, whereby cybercriminals intercept data as it is transmitted from customers to small businesses. Encryption, according to the participants, can be one method of preventing social media cyberattacks.

Firewall

A firewall is a network security device that monitors traffic to and from a network. Firewalls serve as a layer of protection by allowing business leaders visibility regarding network traffic and visitors (Alotaibi & Vassilakis, 2023). Seven participants (P1, P2, P3, P5, P7, P9, and P10) spoke about the importance of having a firewall. P9 described the importance of a firewall saying, “Make sure that whenever you’re employing something into your business, make sure that you’re going to have that firewall that’s going to not allow those customers or those hackers to come in and take something from you.” P9 explained that a firewall can prevent unauthorized access from anyone, including customers. P5 explained that the benefits of a firewall outweigh the costs associated with buying a firewall:

> It’s fairly reasonable for most businesses to have a firewall. They’re not that crazy expensive. If you violate HIPAA compliance, it’s like 50 grand a pop per violation, which is huge for a small business. That can shut down a whole business. It’s reasonable and expected for risk management purposes in your business to have a firewall.

P5 explained that a firewall is necessary for small businesses that must comply with HIPAA laws, and the cost of a firewall is much less than the cost associated with HIPAA violations. Therefore, another mechanism the participants used to deter social media cyberattacks were to purchase a firewall and use it to regularly monitor and protect their systems.

Geotagging

Geotagging was the third strategy the participants used to deter social media cyberattacks. Geotagging is the process of assigning geographic coordinates to media based on the location of the originating device (Khatoon et al., 2022). Two participants (P2 and P5) described taking advantage of geotagging provided by social media sites. P2 observed geotagging as a security measure. P2 described,

> This IP address doesn't line up with where you normally log in from. That's a common security feature enabled on a lot of systems, geotagging. Social media will say, hey, you're using a password from six months ago or nine months ago. This isn't the right password, it flags that, and it helps to make sure that you're the person supposed to be getting in.

P2 carefully observed geotagging messages provided by social media as an alert mechanism for when an intruder accesses the account. P5 also uses geotagging to understand unauthorized access to their accounts. P5 explained,

> Most times, we can back trace them and find them through Geo IP and IP tracing and get a general location where they're at. Sometimes people know who the people are, who are trying to attack them. A lot of times, not, because it's from somebody overseas.

P5 believed that using geotagging of IP addresses can elucidate the nature of a cybercriminal as local, domestic, or international, providing the small business leader with valuable information about the nature of a cyberattack. Thus, geotagging is an important method that some participants used to prevent authorized access to accounts, as it allows small retail business owners to view the locations of individuals accessing their systems.

Limit User Access

Five participants (P1, P2, P4, P6, and P9) discussed limiting user access to social media accounts. For instance, P1 said, “We limit the access to that website. That’s only open to me, my wife, and we hired a person to help with the aesthetics.” P1 conducted business on their website and limited employee access to help prevent unauthorized access and social media attacks. P1 further explained, “We make sure to limit what’s accessible as far as our account when we’re on the Wi-Fi system.” Limiting access to social media accounts and customer information allowed P1 to help deter social media cyberattacks. P9 described limiting access as well. P9 explained, “If you’re on social media sites, make sure that the networks are secure, making sure that the people, the only admins who are using the system, are the ones who are authorized.” Thus, the participants described ensuring that only authorized users and stakeholders have access to company data and systems as an important mitigation factor for social media cyberattacks.

Monitoring

Several participants (P1, P2, P5, P6, P7, P9, P10, and P11) described constant monitoring of systems as an important mechanism to deter social media cyberattacks. P1 conducted daily scans of their systems. P1 said, “We monitor the website for the company, updating the website and also daily reviews of our reports, I make sure to conduct daily scans.” P1 uses daily monitoring to ensure that only authorized users are accessing company information. P10 also described using constant monitoring of systems. P10 said,

> I am tracking all the inbound and outbound traffic on my network. I’m always running Port Scans to make sure that if there are any open ports, I’ll be notified, and I’m constantly monitoring my reports. I also run Wireshark on my network.

P10 monitors their network for open ports, meaning that an individual is using a port to access their network or systems (see Birkinshaw et al., 2019). The monitoring system described by P10 allows for an integrated diagnostic and monitoring of the capacity of ports. Like P10, P3 uses a monitoring system to determine unauthorized access. P3 described,

> We do implement several strategies, [with] the main one being what’s called an EDR system, which monitors the network for them. And that’s an endpoint and response time, endpoint detection, and response time. And so that utility allows us to mimic or watch for any behaviors that may be malicious.

P3 invested in software to help monitor their system, which they believed was an important mitigation factor for social media cyberattacks. These findings indicate that some small retail business owners use consistent monitoring and monitoring systems to deter social media cyberattacks.

Password Security

One of the major recommendations from the participants was to practice good password security. Cybersecurity experts indicate that passwords should be at least 10 characters, containing uppercase and lowercase letters, numbers, and special characters (Curry et al., 2019). According to Zwilling et al. (2022), the lack of adequate password security is the most significant contributor to cyberattacks and social media cyberattacks. The participants' success in mitigating social media cyberattacks may be attributed to diligent password behaviors.

Reset Passwords. Cybersecurity experts suggest resetting passwords every 30 days (Pearman et al., 2019). Four participants (P2, P5, P8, and P10) stressed the importance of resetting passwords frequently. P10 explained, "Usually, the fix is to reset passwords. Clear out all your passwords, redo everything, and then you're usually okay." P10 advocates for resetting passwords to prevent social media cyberattacks. P5 agreed with industry standards regarding changing passwords every 30 days. P5 said, "Obviously, the first layer there is, going as far as being proactive, is changing your passwords on a 30-day basis or weekly basis." P5 recommended changing passwords at least every 30 days, which is consistent with industry recommendations.

Strong Passwords. In addition to resetting passwords, the participants recommended creating strong passwords. P8 described the process of selecting a strong password, saying,

> One of the most obvious or common issues is reusing passwords, we inform them that using the same password multiple times is not a smart idea. So, we try to advise if you’re going to use a password to make it unique for yourself. Making a unique password is always the most recommended thing.

P8 indicated that they advised customers to create unique passwords that another individual could not easily discern. P10 similarly explained that “I constantly remind them that in those days of having no simple passwords, that’s the main thing, you must have a complex password.” P10 stressed the complexity of passwords as a mechanism to increase password strength. P7 also believed that strong passwords prevent cyberattacking, concurring with P8 and P10 about password uniqueness and complexity. P7 described, “Use a strong password. We encourage customers to use all strong passwords whenever they’re making their accounts. And the same thing goes for employees. So all of our employee-based logins have a complex, unique password.” Based on these findings from the participants’ responses, favorable password behaviors, including making strong passwords and resetting them frequently, aid in deterring social media cyberattacks.

Separate Personal and Business Affairs

A common thought among participants was that employees should separate personal and business affairs. Cybersecurity experts suggest that employees should not use their personal devices to conduct business (Furnell & Shah, 2020). Two participants (P4 and P10) spoke explicitly about the need for employees to separate business and personal transactions and communications. P10 explained, “Let’s say employees, I don’t want them on my computers doing personal business. Going through the 2000s, we would see soldiers or employees on their computers checking Facebook or Myspace or doing a transaction on the computer." P10 believed that businesses were more prone to social media cyberattacks when employees were lax regarding the separation of business and personal transactions. Consequently, a company policy of P10 is that no personal transaction can occur on company computers; this policy was examined during the document analysis phase of data analysis. P4 also spoke about the need to separate personal time from business time, stressing that employees sometimes transfer lax behavior to their place of employment. P4 said, "An employee may have a password that's last name123 on their personal device, and if they access my system on their device, I'm vulnerable." P4 noted that vulnerabilities can be transferred from a personal device to a business site if employees do not have good passwords. Consequently, P4, like P10, has an employment policy whereby employees cannot conduct business on their personal devices. Therefore, one method small retail business owners use to mitigate social media cyberattacks is to encourage or require employees to separate their personal and business transactions.

Software Updates

Eight participants (P1, P3, P4, P5, P7, P8, P9, and P10) described ensuring software was properly updated as an important cybersecurity practice. Outdated software can lead to system vulnerabilities for social media cyberattacks (Chigada & Madzinga, 2021). The participants stressed the importance of regular software updates. P3 succinctly said, "Most times, bad hacks happen because of outdated software." P5 found that customers with outdated software are more prone to cyberattacks. P4 explained, “You’ve clients that don’t know their equipment or system is outdated. You got to go in there and tell them, hey, we got to update this because you’re going to keep getting hacked.” P4 concurred with P5 regarding the propensity of customers to encounter cyberattacks based on their use of outdated software or hardware.

Other participants explained the necessity of regular software updates. P7 described, “Regular software updates and patches are applied. So just make sure that there are no vulnerabilities because every single day, there’s always going to be an update.” P7 ascertained that regular software updates prevent vulnerabilities that can lead to social media cyberattacks. P9 also identified regular updates as an important mechanism to address vulnerabilities. P9 said, “Regularly update your system. We often have outdated information and different, outdated systems, which makes you way more vulnerable for someone to attack your system.” P9 stressed the importance of updating systems, which can make it more difficult for cybercriminals to penetrate. Therefore, another mechanism small retail business owners use to mitigate social media cyberattacks is regularly updating their systems.

Two-Factor Authentication

Authentication processes restrict malicious users from accessing data. In authentication, a user or device must prove its identity to the server or client to gain access to a service or data (Deebak & Al-Turjman, 2021). Two-factor authentication is the process by which a user must enter a password and authenticate using another means, such as text message, fingerprint, or face scan (Papaspirou et al., 2021). The participants described using two-factor authentication methods to deter social media cyberattacks. P2 explained,

> Two-factor authentication. Whenever you log in, having a secondary thing that makes you either have an authenticator app that changes codes every 30 seconds, a text message-based system or an email-based system, anything that requires a second additional layer of access is the biggest thing that protects our business and other businesses from being targeted for cyberattacks.

P2 believed that two-factor authentication helps prevented authorized access by providing an extra layer of security to access a system or account. P9 also spoke about two-factor authentications as a mechanism of protection against social media cyberattacks. P9 said, "We use two-factor identification systems. We use a system called Acer, where you'd have to go in with your phones, and they send a password to your phone to verify that you are that person on any network." The participants described using two-factor authentication as a layer of security to prevent unauthorized access to their systems.

Virus or Malware Software

The final method of deterring social media cyberattacks discussed by the participants was using virus or malware software. Virus or malware software detects potential viruses or malware and isolates and destroys them. The participants stressed the importance of obtaining virus and malware software and maintaining them through regular updates. P10 used a variety of software to identify viruses and malware. P10 said,

> I have content filtering, malware, and other software that's built into the firewall that helps me identify vulnerabilities on my network. Without having that in

> place, then I’m quite sure that all types of things that I even read and see about different tags will probably be happening to my network.

P10 believed that virus and malware software was a first line of defense against common social media cyberattacks. P2 also discussed the importance of virus or malware software, saying, “Antivirus software is usually a very important component of the cybersecurity stack. Having a baseline antivirus is important on any machine. It doesn’t prevent everything, but it helps.” P2 noted that the antivirus software helps prevent social media cyberattacks. Therefore, purchasing software aimed at viruses and malware is another method that the participants used to mitigate or deter social media cyberattacks.

Analysis of Theme 1 Under GST

The chosen theoretical framework for this study was GST. GST contains three concepts: (a) system units, (b) continuous interconnectivity, and (c) analyzing systems provides an understanding of interconnected systems (von Bertalanffy, 1972). System units involve systems science, which explores and theorizes systems across various fields. In this study, a system unit is an individual device or a participant’s network. A potential cybercriminal is also a systems unit, an outside system trying to gain unauthorized access to the data or information maintained by a small business. The second aspect of GST, continuous interconnectivity, refers to connections between different system units (von Bertalanffy, 1972). The participants addressed continuous interconnectivity when discussing how one device’s infection can alter an entire network. This concept was evident in the discussion of separating personal and business activities and transactions. The participants described how personal devices and social media accounts could allow unauthorized access to business systems.

The third concept in GST involves an analysis of the systems. The participants spoke to systems analysis extensively in the discussion of Theme 1. The participants described a need for constant monitoring of systems, user access, and employee use of systems. Constant monitoring allows for the analysis of connections between two systems, namely the cybercriminal and the small business devices. Components of constant monitoring include resetting passwords, regularly updating systems software and hardware, and monitoring antivirus and malware software. Therefore, the participants described aspects of systems theory when discussing how to deter social media cyberattacks.

Understanding GST allows individuals to ascertain connections between systems. Perhaps the most striking finding of Theme 1 is the participants' use of multiple mechanisms to prevent social media cyberattacks. All the participants used at least three strategies to deter social media cyberattacks. See Table 3 for a description of the number of strategies used by each participant.

Table 3

Each Participant Used Multiple Prevention and Mitigation Strategies

Participant	No. of Strategies	Strategies
P1	6	Firewall, Limit user access, Monitoring, Software updates, Strong passwords, Virus and malware software
P2	9	Encryption, Firewall, Geotagging, Limit user access, Monitoring, Reset passwords, Strong passwords, Two-factor authentication, Virus and malware software
P3	4	Firewall, Software updates, Two-factor authentication, Virus and malware software
P4	4	Encryption, Limit user access, Separate personal and business affairs, Software updates
P5	8	Encryption, Firewall, Geotagging, Monitoring, Reset passwords, Software updates, strong passwords, Virus and malware software
P6	3	Limit user access, Monitoring, Virus and malware software
P7	5	Encryption, Firewall, Monitoring, Software updates, Strong passwords
P8	4	Reset passwords, Software updates, Strong passwords, Two-factor authentication
P9	7	Firewall, Limit user access, Monitoring, Software updates, Strong passwords, Two-factor authentication, Virus or malware software
P10	8	Firewall, Monitoring, Reset passwords, Separate personal and business affairs, Software updates, Strong passwords, Two-factor authentication, Virus and malware software
P11	3	Monitoring, Strong passwords, Virus and malware software

The use of multifaceted approaches to a problem is inherently a systems approach (von Bertalanffy, 1972). These findings indicate that GST is an appropriate framework for understanding strategies to deter social media cyberattacks by small retail business leaders.

Analysis of Theme 1 in the Context of Existing Literature

In the literature review presented in Section 1, I outlined common strategies employed by small retail business owners. A first strategy was to purchase some type of security software. Firms lacking actionable software inventory are more likely to be attacked by cybercriminals (Kantheti & Manne, 2022). The participants in this study described using firewalls and antivirus and malware software. However, the participants also described such software as cost-prohibitive at times. These findings are consistent with those in the literature, indicating that small retailers with fewer resources than large retailers are often at higher risk for cyberattacks (Alahmari & Duncan, 2020). Thus, the participants corroborated findings in the literature regarding the use of cybersecurity software.

Scholars also suggest that **s**mall retail business leaders should invest in email security to protect their firms, employees, and customers from email security risks. While email technology is indispensable to most businesses (Lallie et al., 2021)., email is often used to send malware, spam, and phishing attacks (Yu, 2020). Industry experts indicate that small retail business leaders should implement aggressive spam filtering so malicious and spam emails do not appear in the user's inbox (Mohammad, 2020). In this study, the participants spoke about email security in the context of making strong passwords, ensuring only authorized access using two-factor authentication and resetting passwords frequently.

A finding in the literature unaddressed by participants was that of cyber insurance. Cyber insurance can cover unexpected costs associated with cybercrimes.

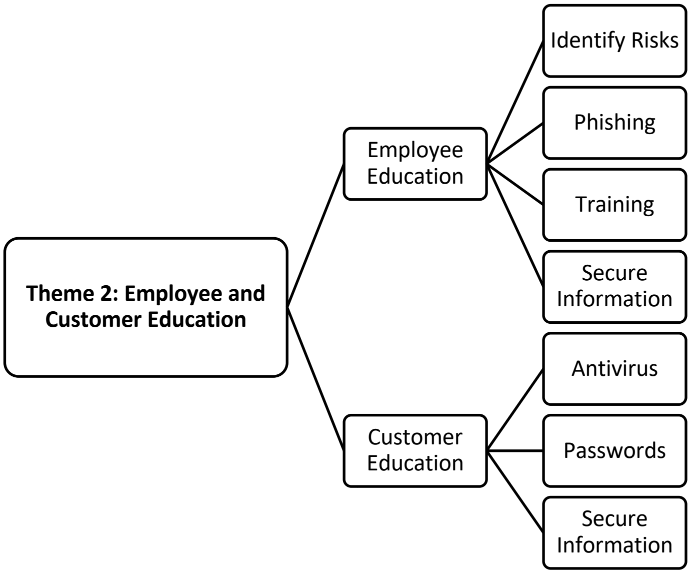
Cyber liability insurance is a good way for small retailer leaders to protect their firms from breaches (Gunduz & Das, 2020). Many companies purchase cyber liability insurance policies to protect their firms from cybercrime or data breaches (Lemnitzer, 2021). However, cyber insurance can be expensive. The participants in this study may have opted for different strategies, such as geotagging and limiting user access, over a more expensive strategy, like cyber insurance, due to limited resources.

Theme 2: Educating Employees and Customers About Social Media Cyberattacks

The second theme elucidated from the participants' interviews was the importance of educating employees and customers about social media cyberattacks. This theme directly contributes to the study's research question because the participants described employee and customer education as an essential prevention strategy. The codes that contribute to this theme are shown in Figure 2.

Figure 2

Codes Contributing to the Development of Theme 2



The participants identified employee education and customer education as an important strategy they use to deter social media cyberattacks.

Employee Training

The strategy for deterring social media cyberattacks most frequently mentioned by the participants was employee training. P1 administers a training class aimed at educating employees about cybersecurity protocols and best practices. P1 said,

> It's just to have good controls and make sure that your employees are trained. We've had to, actually, one day close the shop. And we did a little class with all our employees. We have to teach them that not everybody knows how to use these systems. So, teaching them how to make sure that the software is working, that the virus software is on and that they're also trained to be able to do the job.

P1 found that not all employees knew best practices regarding cybersecurity and weren't aware of how to operate antivirus software properly. P1 attempted to remedy this problem through an employee training day. P11 also found that not all employees were educated regarding phishing incidents. P11 said, "We try to inform everybody of what's going on with certain situations. We make sure employees know what to do and what not to do in situations of unknown people sending links and trying to get to our systems." P11 described needing to educate employees regarding phishing schemes and unauthorized access, which may not always be obvious.

Other participants described employee training as an essential mitigation technique for social media cyberattacks. P2, like P11, found that their employees could not identify a social media cyberattack. P2 said, "Educating staff and employees that are interacting with it to know what an attack looks like is a huge thing. We have to take an hour block of time to just go over the most common things." The participants have found that, in their experience, their employees are not all aware of common social media cyberattacks, and without adequate training on attack identification and mitigation, employees cannot respond appropriately to potential threats. P7 also described extensive employee training. P7 said, "We conduct regular training sessions to educate employees about the importance of security and potential risks. Basically, teaching them how to identify and report suspicious activity if they noticed anything's off, practicing good password hygiene." P7 educated employees regarding different aspects of cybersecurity, including password behaviors and how to recognize suspicious activity. Therefore, one mechanism by which the participants deter social media cyberattacks is through proper employee training regarding cybersecurity, as well as the risks associated with social media and cyberattacks.

Customer Training

Many of the participants operated computer repair or consulting businesses. These participants discussed the importance of educating customers regarding social media cyberattacks. P6 found that customers didn't understand that virus software requires subscription renewal. P6 said, "We educate the customer when they're coming to pick up what virus we put on when the free trial ends and if they need to activate it. I like to educate people as much as I can when it comes to the internet." P6 believed that customers should be educated regarding best practices in cybersecurity and on the internet, which is essential in preventing repeated social media cyberattacks. P9 also described educating customers regarding how to secure their information. P9 said, "We educate customers about important information that can be secured online because you want to avoid any type of issues when it comes to people trying to attack your system." P5 also educated customers, noting, "If it's a home user, we're not going to the FBI with this. All you can do is try to educate them as far as what they did wrong and what needs to be corrected." P5 spoke to the inevitability and commonness of social media cyberattacks, which often cannot be addressed by authorities on a small scale. Consequently, P5 advocated for customer education regarding best practices in cybersecurity. Therefore, the participants described customer training as an essential strategy for deterring social media cyberattacks.

Analysis of Theme 2 Under GST

By using employee and customer education as a strategy to mitigate social media cyberattacks, the participants described a systems theory approach. Devices, applications, and personnel are all essential components of a system in the context of cybersecurity (Pollini et al., 2022). By recognizing the importance of employee and customer education, the participants underscored the importance of each individual as a causal agent and partner regarding issues of cybersecurity. The improper password hygiene or lax security measures of one employee can create a risk that is transmitted to a device or an entire system (Baraković & Baraković Husić, 2022). Therefore, the participants' emphasis on employee and customer training is an important aspect of systems theory regarding cybersecurity and applied to social media cyberattacks.

Analysis of Theme 2 in the Context of Existing Literature

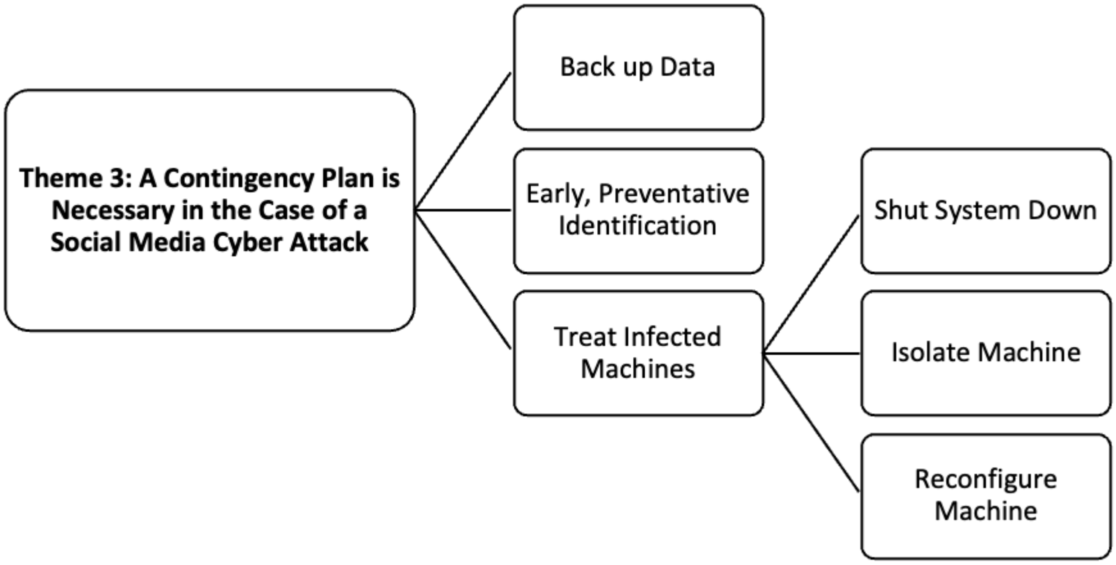
Employee behavior and training was a prevalent topic in the cybersecurity literature. Cybersecurity experts suggest that training employees on cybersecurity can resolve one of the greatest weaknesses of any organization: the human factor. By comprehending and applying cybersecurity best practices, employees can become the first line of defense against cyberattacks (Buresh & Esq, 2022). Small retail businesses leaders can tailor training programs to their particular requirements and priorities (Devi, 2023). Industry experts suggest that regular training updates and refreshers can help maintain a high level of cybersecurity awareness among employees (Y. Li et al., 2020). This continual education fosters a culture of vigilance, highlighting the significance of cybersecurity in daily operations.

Theme 3: A Contingency Plan is Necessary in the Case of a Cyberattack

The small retail business owners interviewed in this study described having a contingency plan as a requirement in the case of a social media cyberattack. This theme directly contributes to the study's research question by providing a set of contingency strategies that some small retail business leaders use in response to social media cyberattacks. The codes that contributed to this theme are shown in Figure 3.

Figure 3

Codes Contributing to the Development of Theme 3


Theme 3: A Contingency Plan is Necessary in the Case of a Social Media Cyber Attack
Back up Data
Early, Preventative Identification
Treat Infected Machines
Shut System Down
Isolate Machine
Reconfigure Machine

The participants considered three components as essential elements of a contingency plan: (a) backup data, (b) early, preventative identification, and (c) treat infected machines. The participants' thoughts regarding these components of their contingency plans are now discussed.

Back-Up Data

The participants (P2, P3, P7, P10) described data back-ups as an essential component of a contingency plan. P2 described the importance of having data backup in case an attack occurred. P2 said, "Some of the businesses we deal with had backups, and the backup were not affected. So, we just pulled the back-ups and restored their data, and secured the network." P2, a leader of a computer repair company, demonstrated that when customers have a backup of their data, P2 is able to effectively help restore a customer's system. P3 also discussed using backups in the case of an attack. P3 said,

> It's a situation where the first thing is to make sure we have study backups. We also do study backups locally, as well as in the cloud. At the end of the day, no solution is 100% not hackable. When what we can do is try to prevent as much as we can. The best thing at that point we can do is just to restore the data. Revert the situation, find out exactly what hold they came in through, and try to block that.

P3, like P2, uses a data backup as a contingency plan in the case of a cyberattack. They explained that the infected system could be restored using a data backup with little disruption to business operations. P7 also described the necessity of data back-ups in terms of minimizing downtime after a cyberattack. P7 said, "In the hopes of trying to recover, we have a backup system in place to restore the data and minimize any downtime for the customer or us." P7 elucidated that a backup system allows them to minimize disruptions to business operations after a social media cyberattack. Thus, one element of a successful contingency plan is regular data backups.

Early Preventative Identification of Vulnerabilities

Participants P9 and P10 discussed early preventative identification of weaknesses as essential to a successful contingency plan. P9 explained,

> I think, also, you just want to identify those weaknesses. You guys want to make sure that there's no potential entry point for an attacker to come in and destroy anything that you may have. Just that information about weaknesses.

P9 explained that an essential component of a contingency plan is knowing the weaknesses and vulnerabilities associated with the system. Knowing weaknesses allows for contingencies to be made in the eventuality that a cyberattack does occur. P10 also believed in preventative measures. P10 described,

> I do a little research and try to see where that vulnerability or that risk is generated from so I can adjust in the future. I also have access to a couple of other portals that give me information on to see how that risk has affected other businesses. This gives me insight into what I may need to fix.

Like P9, P10 believed that understanding risks and vulnerabilities in their system was an important aspect of risk management and a contingency plan in the case of a social media cyberattack. Therefore, a second aspect of a contingency plan is the early, preventative identification of weaknesses and vulnerabilities.

Treat Infected Machines

The main component of the participants' contingency plan was to treat infected machines or devices. Within the context of treating infected machines, the participants recommended shutting down the system and isolating and reconfiguring an infected machine. P1 suggested beginning with shutting down their system, saying, "The contingency plan is limited based on our size. I mean, the best we can do is to shut the system down." P1 highlighted that as a small retail business leader, resources are limited, rendering a shutdown as the most economical and plausible option in the case of a social media cyberattack. P2 concurred with P1, noting that the first line of defense against a cyberattack is to shut down the system. P2 said,

> You have to shut it down. That’s the biggest thing. Disconnecting from the internet will cause a lot of things to happen when you’re under a cyberattack, Number one, they can no longer access you. So, you just unplug your router that will at least stop what’s happening at the moment. No more data can go out and no more data can go in, right? So, in this situation, if my business is under attack, I’m going to disconnect everything.

P2 highlighted that disconnection of the system from the internet can prevent further damage from occurring in the case of a social media cyberattack. Other participants, including P3, P5, and P8, all reiterated similar thoughts regarding removing the infected system from the internet during a cyberattack.

Some participants spoke about the need to isolate an infected device or machine. For instance, P5 described needing to isolate an infected machine. P5 said, “But really, the best thing is to cut the cord, isolate the computers and servers that you know have been affected.” P5 identified machine isolation as a component of their contingency plan. P4 uses machine isolation as a strategy to prevent social media cyberattacks. P4 explained,

> Security-wise, each computer is isolated from the other, and there’s no data stored on these computers. We don’t store any credit card information. So, in and of itself, if you took the average hacker and they got into a computer or laptop, if they were able to get access, it would be pretty innocuous and pretty boring in a very unattractive target.

Not only is machine isolation important in the event of a social media cyberattack but isolating machines and devices can be an effective security measure, according to P4.

After an infected machine has been identified an isolated, the participants recommended reconfiguring the machine and restoring previous settings. P2 said, “Obviously, reimaging all machines is mandatory after a ransomware attack. Every machine needs to be wiped and reinstalled with fresh windows. You do not know what is or isn’t good on that drive.” P2 believed that machine reconfiguration is a necessary step, as the targeted drive or application of a social media cyberattack is not always obvious. P8 also advocated for machine reconfiguration in conjunction with resetting passwords and restoring previous account settings. P8 said,

> We would log out of every device that we have, get our recovery, probably go to the safe, go get our recovery passkey to try to get access back into our account, purge every account and every device that has access, manually reset everything, and reconfigure all machines.

Thus, an important aspect of a contingency plan after a social media cyberattack is reconfiguring infected machines after they have been identified and isolated.

Analysis of Theme 3 Under GST

In Theme 3, the participants discussed important aspects of their contingency plans in the case of a social media cyberattack. The important components of their contingency plans include: (a) creating regular data back-ups, (b) early preventative measures, and (c) treating infected machines. The participants’ contingency plans are consistent with a GST framework. By backing up the data on each individual machine, the participants underscored the interconnectedness of each device on a network. Regular data backups on individual machines allow for data to be stored in a secure location on a network, thereby preventing data loss (Logeshwaran et al., 2023). The identification of early and preventative assessment of weaknesses and vulnerabilities highlights the participants' understanding that an outside system, namely cybercriminals, influences their own systems. This concept is inherent to a systems approach, as the participants considered an outside system in conjunction with their own systems. Finally, the participants described the importance of shutting down their systems and isolating an infected machine during a cyberattack. In isolating an infected machine, the participants noted their understanding of the interconnectedness of their systems. An infected machine can adversely influence other machines in a connected system (Miller et al., 2021). Thus, the participants' contingency plans were derived from an analysis of their entire system, not just one infected machine or account.

Analysis of Theme 3 in the Context of the Existing Literature

Contingency planning for cyberattacks was a common research topic in the literature. Researchers advised that small retail business leaders implement cyberattack contingency planning to mitigate the effects of cyber incidents, safeguard customer data, and ensure business continuity. A well-developed contingency plan outlines the steps to take prior to, during, and following a cyberattack (Kusumastuti et al., 2020). One way researchers have suggested engaging in this practice is to first conduct a thorough risk assessment to identify potential cyber threats and vulnerabilities unique to your organization (Devi, 2023; Y. Li et al., 2020). The participants highlighted the importance of understanding and accessing the vulnerabilities in their systems in conjunction with making regular data backups.

Cybersecurity experts discussed different aspects of contingency planning compared to the participants' ideas. Scholars indicated that small retail business leaders should assemble an incident response team with clearly defined roles and responsibilities (Tam et al., 2021). This team should include members from departments such as IT, legal, human resources, and public relations (Kusumastuti et al., 2020). The participants described their contingency plan as shutting down their system and isolating and treating the infected machine. The participants did not describe having other departments involved in their contingency plans. This finding may speak to the limited nature of financial resources of many small retail businesses.

Application to Professional Practice

The findings of this research study have important significance for the professional practice of small retail business leaders in the United States in their efforts to avoid social media cyberattacks and protect their operations. Cyberattacks have become a major concern due to increased reliance on social media for marketing, client management, and retention (Susanto et al., 2021). This key subsection addresses the study's findings' application and makes a persuasive academic argument for how these findings might lead to better business practices in the field of cybersecurity.

Implementing Comprehensive Cybersecurity Strategies

The theme of employing multiple strategies to prevent social media cyberattacks offers a clear directive for small retail business owners. It emphasizes the importance of moving beyond a single security measure and implementing a holistic cybersecurity strategy. To reinforce their social media accounts, small retail business leaders should invest in strong authentication systems, encryption techniques, and safe access controls (Dahiya et al., 2022). Furthermore, updating software and security systems on a regular basis can considerably lower the likelihood of successful cyberattacks (Purkait & Damle, 2023). The use of multiple cybersecurity strategies and measures is considered a best practice according to industry standards regarding the prevention of social media cyberattacks (Ghelani, 2022). Thus, small retail business leaders should use multiple strategies to deter cybercriminals from engaging in social media cyberattacks with their companies.

Prioritizing Employee and Customer Education

The findings, specifically Theme 2, which focused on staff and consumer education, emphasize the importance of employees' understanding of system vulnerabilities and cybersecurity threats in reducing social media cyberattacks. According to Buil-Gil and Barrett (2022), employee mistakes are the leading cause of cyberattacks in small- and medium-sized enterprises. Small retail business leaders must prioritize cybersecurity training for their employees, teaching them how to identify phishing efforts, fraudulent links, and other social engineering strategies (Ncubukezi et al., 2020; Pawar & Palivela, 2022). At the same time, small retail business leaders should provide instructional resources for clients, supporting safe online practices and ensuring that they do not unintentionally become a route for cyberattacks (AlDaajeh et al., 2022). Customer education is especially important for small retail businesses that operate in the technology industry (Müller, 2019). Small retail business leaders should prioritize employee and customer education to aid in the prevention of social media cyberattacks.

Developing Effective Contingency Plans

The findings emphasize the necessity of a contingency plan when facing a social media cyberattack. While a contingency plan is not a deterrent for social media cyberattacks, it is an essential cybersecurity practice (Datta & Nwankpa, 2021). The participants emphasized the necessity of anticipating social media cyberattacks and planning to minimize the impact on business operations. Small retail businesses are especially vulnerable to cyberattacks when their limited human and financial resources are considered (Aldasoro et al., 2022). Small retail business leaders should develop detailed cyberattack response plans that outline the roles and duties of critical stakeholders such as IT professionals and legal counsel. Such plans should also include communication strategies for transparently dealing with consumers and stakeholders during cyberattacks.

Implications for Social Change

The findings of this research study hold profound implications for driving tangible improvements in individuals, communities, organizations, institutions, cultures, and societies by enhancing cybersecurity practices among leaders of U.S. small retail businesses. Specifically, identifying numerous tactics employed by small retail business owners to prevent social media cyberattacks empowers these leaders to protect their businesses proactively. Leaders may better secure their organizations and consumer data by deploying various cybersecurity measures, lowering the likelihood of successful cyber invasions (R. Chen et al., 2021; Kipper et al., 2021). Furthermore, prioritizing cybersecurity education for employees and consumers develops an awareness culture within these organizations. Research also shows that employees who are more educated are better able to identify and respond to possible dangers, while customers become more responsible online users (Grewal et al., 2020). This cultural shift safeguards enterprises and leads to a more secure digital environment for all.

Acknowledging the need for contingency planning in the face of cyberattacks emphasizes the need for preparedness in the corporate sector. Business leaders can secure their operations and sustain profitability by taking proactive and resilient steps to prevent social media cyberattacks (Devi, 2023). Furthermore, a focus on collaboration among small retail business leaders develops a sense of mutual support and encourages the exchange of expertise, best practices, and resources. This joint strategy can help forge a more formidable front against cyber enemies, enhancing customer trust and confidence in online transactions (Saura et al., 2021). These implications create chances for social change as small retail business leaders become change agents, contributing to a better and more secure digital ecosystem for all stakeholders.

Recommendations for Action

Using GST as a framework for the analysis in this study, I identified three themes that emerged from the participants' interviews. The participants described using multiple strategies to deter social media cyberattacks (Theme 1), including employee and customer education (Theme 2). The participants also identified the need for a contingency plan, which involved creating data backups and understanding vulnerabilities (Theme 3). Analysis of these findings using GST as a framework allows for the integration of these themes into a comprehensive set of strategies for deterring social media cyberattacks, as shown in Figure 4.

Figure 4

A Systems Theory Approach to Deterring Social Media Cyberattacks

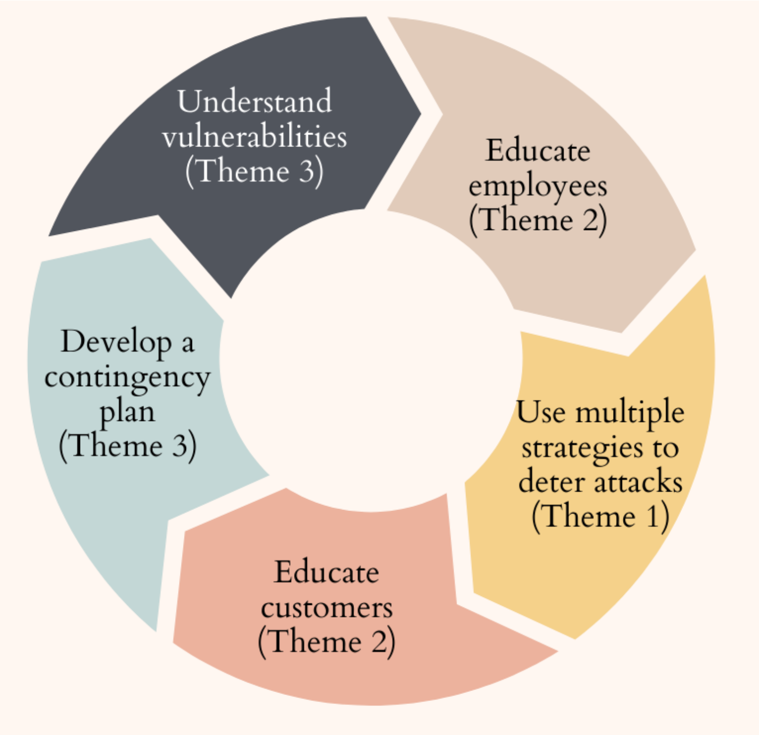

Understand vulnerabilities (Theme 3)
Educate employees (Theme 2)
Use multiple strategies to deter attacks (Theme 1)
Educate customers (Theme 2)
Develop a contingency plan (Theme 3)

Figure 4 presents a visual representation of the comprehensive set of strategies for deterring social media cyberattacks, derived from the analysis of the study's findings using the GST as a framework. Participants described that small companies should use multiple strategies to deter attacks, educate customers, educate employees, develop a contingency plan, and understand vulnerabilities.

Building Collaboration and Information Sharing

Figure 4 highlights that using GST as an approach to understanding strategies used by small retail business leaders to mitigate social media cyberattacks allows for the development of an integrate cybersecurity framework. Individual efforts may need to be more sufficient in properly securing against cyberattacks in an era where cyber threats are becoming increasingly complex and persistent (Susanto et al., 2021). As a result, industry collaboration has emerged as a critical aspect in the quest for improved cybersecurity standards (Mijwil et al., 2023). Small retail business leaders should proactively solve their cybersecurity challenges by building strategic alliances and networks with leaders of other small and larger enterprises (Ding et al., 2018). They may share their expertise, experiences, and information by collaborating to confront developing cyber threats. This collaborative approach enables firms to benefit from various viewpoints and insights, promoting a culture of shared learning and collective problem-solving.

The exchange of best practices is a critical component of this joint effort. Through these collaborations, small retail business leaders can learn from one another’s triumphs and failures in dealing with cyber disasters. They can identify novel cybersecurity strategies that might not have been obvious in isolation (Buresh & Esq, 2022). This ongoing knowledge-sharing gives each community member the skills and understanding they need to improve their cybersecurity posture. Furthermore, these collaborative endeavors can include resource pooling (Devi, 2023). In the face of limited resources, small retail business leaders can pool their resources to invest in cybersecurity solutions, services, and training programs that would otherwise be prohibitively expensive

(Azubuike, 2021; Y. Li et al., 2020). The research shows that by sharing the financial burden, businesses can obtain cutting-edge technologies and specialized services that efficiently enhance their defenses against cyberattacks.

Emphasizing a community-driven approach to cybersecurity can have far-reaching consequences beyond organizations, which also has implications for positive social change. The findings indicate that a unified front of small retail business leaders can enhance their voice and influence in campaigning for regulatory reforms and actions to combat cybercrime on a bigger scale. Policymakers and law enforcement agencies are more likely to notice a coordinated effort from a group with a common goal and a commitment to strengthening cybersecurity standards (Gulyas & Kiss, 2023; Udofot & Topchyan, 2020). A community-driven approach to cybersecurity, where small retail business leaders collaborate through strategic alliances and knowledge-sharing, allows for the development of an integrated cybersecurity framework, resource pooling, and the potential to advocate for regulatory reforms and actions against cybercrime on a larger scale.

Recommendations for Further Research

This qualitative case study on strategies used by U.S. small retail business leaders to deter social media cyberattacks has provided valuable insights into the cybersecurity practices of this specific group. However, there are several areas that could benefit from further investigation to expand and strengthen the knowledge in this domain. The following five recommendations for further research are suggested:

1. Exploring cybersecurity practices in larger retail enterprises; while this study focuses on small retail organizations, comparative research to understand the cybersecurity techniques implemented by larger retail enterprises would be beneficial. Examining the contrasts and similarities in tactics used by small and large organizations can provide a more comprehensive view of effective cybersecurity procedures in the retail industry.
2. Investigating the impact of cybersecurity education programs; exploring cybersecurity practices in larger retail enterprises; while this study focuses on small retail organizations, comparative research to understand the cybersecurity techniques implemented by larger retail enterprises would be beneficial. Examining the contrasts and similarities in tactics used by small and large organizations can provide a more comprehensive view of effective cybersecurity procedures in the retail industry.
3. Investigating the impact of cybersecurity education programs; exploring cybersecurity practices in larger retail enterprises; while this study focuses on small retail organizations, comparative research to understand the cybersecurity techniques implemented by larger retail enterprises would be beneficial. Examining the contrasts and similarities in tactics used by small and large organizations can provide a more comprehensive view of effective cybersecurity procedures in the retail industry.
4. Examining the influence of industry collaboration, the study discussed the possible advantages of corporate collaboration in strengthening cybersecurity

defenses. Future research might investigate the extent to which small retail enterprises collaborate in sharing cybersecurity expertise, resources, and best practices. It would also be interesting to examine how industrial associations or partnerships affect cybersecurity resilience.

5. Examining cross-cultural perspectives on cybersecurity in retail businesses; this study focused on small retail firms in the United States. However, cybersecurity challenges and strategies may differ depending on the cultural setting. Exploring and learning how firms in various cultural settings approach cybersecurity can provide a global perspective on effective cybersecurity procedures.

This qualitative case study has paved the way for understanding the measures utilized by small retail business owners in the United States to discourage social media cyberattacks. To advance the field of cybersecurity in this context, additional research should look into different aspects of cybersecurity practices, broaden the scope to larger enterprises and diverse cultural settings, and use both qualitative and quantitative methods to gain a better understanding of effective cybersecurity strategies. By addressing these research recommendations, scholars and practitioners can collectively contribute to enhancing cybersecurity resilience in the retail industry and safeguarding businesses and customers from cyber threats.

Reflections

As a cybersecurity professional, I had an interest in understanding the cybersecurity mechanisms that small retail business leaders use to prevent social media cyberattacks. As a member of the U.S. Army working in cybersecurity, I understand the importance of cyberattack mitigation strategies. Thus, I had extensive cybersecurity knowledge prior to conducting this study. However, as a government official, I had an incomplete understanding of cybersecurity mechanisms and protocols used in the private sector, which must be inherently different from those used in the public sector. This lack of knowledge prompted my interest in the research topic, as I may become a small retail business leader myself after my retirement from the U.S. military.

I do not believe that my preconceived notions about cybersecurity influenced the views of the participants. The participants spoke freely about their cybersecurity mechanisms and protocols. My cybersecurity knowledge allowed me to ask prompting questions when necessary and clarify cybersecurity terms for the participants. Conducting this study allowed me to expand my knowledge regarding cybersecurity in the private sector, especially applied to small retail businesses. I learned that many of the same strategies apply in the public and private sectors, including the need for diverse strategies to mitigate social media cyberattacks.

Conclusion

This qualitative multiple-case study utilizing GST revealed that successful U.S. small retail business leaders employ multiple strategies to prevent social media cyberattacks, prioritize employee and customer education, and develop effective contingency plans. Implementing comprehensive cybersecurity strategies, prioritizing education, and planning for contingencies is critical for small retail business leaders to protect their businesses in an era of increasing cyber threats (Gulyas & Kiss, 2023;

Kusumastuti et al., 2020). Furthermore, by adopting a community-driven approach to cybersecurity through collaboration, knowledge-sharing, and resource pooling, small retail business leaders can strengthen their defenses against cyberattacks and advocate for regulatory reforms to combat cybercrime on a larger scale (Azubuike, 2021). The study's findings have implications for positive social change by fostering a secure digital ecosystem and encouraging responsible cybersecurity practices. Additionally, further research is recommended to explore cybersecurity practices in larger retail enterprises, investigate the impact of cybersecurity education programs, examine the influence of industry collaboration, study cross-cultural perspectives on cybersecurity, and conduct quantitative studies on the financial impact of cyberattacks. These efforts will enhance cybersecurity resilience and safeguard small retail businesses and their customers from cyber threats.

References

Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In *Computational Intelligent Security in Wireless Communications* (pp. 201–220). CRC Press. https://doi.org/10.1201/9781003323426-12

Ahmad, R., & Thurasamy, R. (2021). A systematic literature review of routine activity theory's applicability in cybercrimes. *Journal of Cyber Security and Mobility*, *11*(3), 405–432. https://doi.org/10.13052/jcsm2245-1439.1133

Alahmari, A., & Duncan, B. (2020). *Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020,* pp. 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Alam, M. K. (2021). A systematic qualitative case study: questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management: An International Journal*, *16*(1), 1–31. https://doi.org/10.1108/QROM-09-2019-1825

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences, 34*(10), 8176–8206. https://doi.org/10.1016%2Fj.jksuci.2022.08.003

Alazab, M., Hong, S. H., & Ng, J. (2021). Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Future Generation Computer Systems*, *116*, 22–29. https://doi.org/10.1016/j.future.2020.10.017

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, Article 102754. https://doi.org/10.1016/j.cose.2022.102754

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, Article 100989. https://doi.org/10.1016/j.jfs.2022.100989

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259

Allan, G. (2020). Qualitative research. In *Handbook for Research Students in the Social Sciences* (pp. 177–189). Routledge. https://doi.org/10.4324/9781003070993-18

Alluhaybi, B., Alrahhal, M. S., Alzhrani, A., & Thayananthan, V. (2019). A survey: Agent-based software technology under the eyes of cyber security, security controls, attacks and challenges. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *10*(8). https://doi.org/10.14569/ijacsa.2019.0100828

Al-Musib, N. S., Al-Serhani, F. M., Humayun, M., & Jhanjhi, N. Z. (2021). Business email compromise (BEC) attacks. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.03.647

Alotaibi, F. M., & Vassilakis, V. G. (2023). Toward an SDN-Based web application firewall: Defending against SQL injection attacks. *Future Internet*, *15*(5), 170. https://doi.org/10.3390/fi15050170

ALSaleem, B. O., & Alshoshan, A. I. (2021, March). Multi-factor authentication to systems login. In *2021 National Computing Colleges Conference (NCCC)* (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/9428806

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal of Retailing and Consumer Services*, *68*, 103042–103055. https://doi.org/10.1016/j.jretconser.2022.103042

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). *Measuring the changing cost of cybercrime* [Paper presentation]. The 2019 Workshop on the Economics of Information Security, Boston, MA. https://orca.cardiff.ac.uk/id/eprint/122684

Azubuike, S. (2021). Cybersecurity attacks: Regulatory and practical approach towards preventing data breach and cyberattacks in USA. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3878326

Bahadoripour, S., MacDonald, E., & Karimipour, H. (2023). *A deep multi-modal cyberattack detection in Industrial Control Systems*. *arXiv [cs.CR]*. http://arxiv.org/abs/2304.01440

Baier, A. L. (2019). The ethical implications of social media: Issues and recommendations for clinical practice. *Ethics & Behavior*, *29*(5), 341–351. https://doi.org/10.1080/10508422.2018.1516148

Baltes, S., & Ralph, P. (2022). Sampling in software engineering research: A critical review and guidelines. *Empirical Software Engineering*, *27*(4), 94. https://doi.org/10.1007/s10664-021-10072-8

Baraković, S., & Baraković Husić, J. (2022). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective*, *32*(5), 347–370. https://doi.org/10.1080/19393555.2022.2088428

Belhadi, A., Zkik, K., Cherrafi, A., & Sha'ri, M. Y. (2019). Understanding big data analytics for manufacturing processes: Insights from literature review and multiple case studies. *Computers & Industrial Engineering, 137*, Article 106099 https://doi.org/10.1016/j.cie.2019.106099

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management, 8*(1), 1–10. https://doi.org/10.1504/IJBCRM.2018.090580

Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. *Journal of Network and Computer Applications*, *136*, 71-85. https://doi.org/10.1016/j.jnca.2019.03.005

Bottoms, A. E., & Wiles, P. (1997). Environmental criminology. In M. Maguire, R. Moran, & R. Reiner (Eds.), *The Oxford handbook of Criminology* (pp. 620-656). Clarendon Press. https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=1225989

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative research in Sport, Exercise, and Health, 11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, *13*(2), 201-216. https://doi.org/10.1080/2159676X.2019.1704846

Brooks, C. (2022). Alarming cyber statistics for mid-year 2022 that you need to know. *Forbes.* https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/

Brown, A., & Danaher, P. A. (2019). CHE principles: Facilitating authentic and dialogical semi-structured interviews in educational research. *International*

Journal of Research & Method in Education, *42*(1), 76-90. https://doi.org/10.1080/1743727X.2017.1379987

Buchanan, R. (2019). Systems thinking and design thinking: The search for principles in the world we are making. *She Ji: The Journal of Design, Economics, and Innovation, 5*(2), 85–104. https://doi.org/10.1016/j.sheji.2019.04.001

Buil-Gil, D., & Barrett, E. (2022). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. In *The New Technology of Financial Crime* (pp. 5-34). Routledge.

Buresh, D., & Esq, D. L. (2022). A simulation of how a cloud service provider from the Midwest should behave when faced with a potential cyberattack, where many of its customers do business in the healthcare, banking, and educational industries. *Studies in Social Science Research*, *3*(4), 24. https://doi.org/10.22158/sssr.v3n4p24

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and practice*, *2*, 1-10. https://doi.org/10.1186/s42466-020-00059-z

Caboni, F. (2020). The use of digital technology to reshape the retail store. *International Journal of Business and Management, 15*(1), 149–156. https://doi.org/10.5539/ijbm.v15n1p149

Campbell, R., Goodman-Williams, R., Feeney, H., & Fehler-Cabral, G. (2020). Assessing triangulation across methodologies, methods, and stakeholder groups: The joys, woes, and politics of interpreting convergent and divergent data. *American*

Journal of Evaluation, *41*(1), 125-144. https://journals.sagepub.com/doi/pdf/10.1177/1098214018804195

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of research in Nursing*, *25*(8), 652-661. https://doi.org/10.1177/1744987120927206

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

Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P., Han, Y., Jmila, H., Blanc, G., Takahashi, T., & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: a literature survey. *Annals of Telecommunication, 77*, 789–812. https://doi.org/10.1007/s12243-022-00926-7

Chatterjee, D. (2021). *Cybersecurity readiness: A holistic and high-performance approach*. SAGE Publications. https://doi.org/10.4135/9781071837313

Chatterjee, S., & Kar, A. K. (2020). Why do small and medium enterprises use social media marketing and what is the impact: Empirical insights from India. *International Journal of Information Management*, *53*, 102103–102116. https://doi.org/10.1016/j.ijinfomgt.2020.102103

Chen, R., Kim, D. J., & Rao, H. R. (2021). A study of social networking site use from a three-pronged security and privacy threat assessment perspective. *Information & Management*, *58*(5), 103486. https://doi.org/10.1016/j.im.2021.103486

Chen, Z. F., & Cheng, Y. (2020). Consumer response to fake news about brands on social media: the effects of self-efficacy, media trust, and persuasion knowledge on brand trust. *Journal of Product & Brand Management*, *29*(2), 188–198. https://doi.org/10.1108/JPBM-12-2018-2145

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, *10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11.

Christen, M., Gordijn, B., & Loi, M. (2020). *The ethics of cybersecurity* (p. 384). Springer Nature.

Coburn, A., Leverett, E., & Woo, G. (2018). *Solving cyber risk: protecting your company and society*. John Wiley & Sons.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588–608. http://dx.doi.org/10.2307/2094589

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165. https://doi.org/10.1016/j.compind.2019.103165

Creswell, J., & Poth, C. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed). Sage. https://us.sagepub.com/en-us/nam/qualitative-inquiry-and-research-design/book246896

Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, *27*(3), 871-884. https://doi.org/10.1108/JFC-02-2020-0026

Curry, M., Marshall, B., Correia, J., & Crossler, R. E. (2019). InfoSec process action model (IPAM): Targeting insiders' weak password behavior. *Journal of Information Systems*, *33*(3), 201-225. https://doi.org/10.2308/isys-52381

Dahiya, A., Gupta, B. B., Alhalabi, W., & Ulrichd, K. (2022). A comprehensive analysis of blockchain and its applications in intelligent systems based on IoT, cloud and social media. *International Journal of Intelligent Systems*, *37*(12), 11037-11077. https://doi.org/10.1002/int.23032

Datta, P., & Nwankpa, J. K. (2021). Digital transformation and the COVID-19 crisis continuity planning. *Journal of Information Technology Teaching Cases*, *11*(2), 81-89.

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, *2*(2), 25-36. https://doi.org/10.46809/jpse.v2i2.20

Deebak, B. D., & Al-Turjman, F. (2021). Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future Generation Computer Systems*, *116*, 406–425. https://doi.org/10.1016/j.future.2020.11.010

Deering, K., & Williams, J. (2020). Approaches to reviewing the literature in grounded theory: A framework. *Nurse Researcher, 28*(4), 9–15. https://doi.org/10.7748/nr.2020.e1752

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target, *Telemat. Informatics*, *35*(5), pp. 1277–1287. https://journals.riverpublishers.com/index.php/JCSANDM/article/download/12451/10.1016/j.tele.2018.02.009

Denzin, N. K., & Lincoln, Y. S. (2018). The Sage handbook of qualitative research (5th ed.). Sage.

Devi, S. (2023). Cyberattacks on health-care systems. *The Lancet Oncology*, *24*(4), e148. https://doi.org/10.1016/S1470-2045(23)00119-5

Dias, R. M., Zacarias, R. O., Varella, J. L. D. L., & dos Santos, R. P. (2022). Investigating information security in systems-of-systems. *XVIII Brazilian Symposium on Information Systems* (pp. 1–8). https://doi.org/10.1145/3535511.3535523

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

Dupuis, M., Jennings, A., & Renaud, K. (2021, October). Scaring people is not enough: an examination of fear appeals within the context of promoting good password hygiene. In *Proceedings of the 22nd Annual Conference on Information Technology Education* (pp. 35-40). https://doi.org/10.1145/3450329.3476862

Espinosa, M. R. (2022). Small business cybersecurity: A loophole to consumer data. *The Scholar: St. Mary's Law Review on Race and Social Justice*, *24*(2), 277–334. https://commons.stmarytx.edu/thescholar/vol24/iss2/5

Falco, G. J., & Rosenbach, E. (2022). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press.

Farquhar, J., Michels, N., & Robson, J. (2020). Triangulation in industrial qualitative case study research: Widening the scope. *Industrial Marketing Management*, *87*, 160-170. https://doi.org/10.1016/j.indmarman.2020.02.001

Franck, B., & Reith, M. (2022). Developing mandatory reporting for cyberattacks on U.S. businesses. *Proceedings of the European Conference on Information Warfare and Security*, *21*(1), 70–77. https://doi.org/10.34190/eccws.21.1.308

Franke, U., & Meland, P. H. (2019, June). Demand side expectations of cyber insurance. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1–8). IEEE. https://doi.org/10.1109/CyberSA.2019.8899685

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6–12.

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness?. *Computer Fraud & Security*, *2020*(8), 6-12. https://doi.org/10.1016/S1361-3723(20)30084-1

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1), 19-32. https://doi.org.10.5590/JOSC.2018.10.1.02

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*. https://doi.org/10.22541/au.166385207.73483369/v1

Grewal, D., Hulland, J., Kopalle, P. K., & Karahanna, E. (2020). The future of technology and marketing: A multidisciplinary perspective. *Journal of the Academy of Marketing Science, 48*(1), 1–8. https://doi.org/10.1007/s11747-019-00711-4

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PloS one*, *15*(5), Article e0232076. https://doi.org/10.1371/journal.pone.0232076

Gulyas, O., & Kiss, G. (2023). Impact of cyberattacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

Hai-Jew, S. (2019). Modeling processes and outcomes from cybersecurity talent gaps in global labor markets. *Global Cyber Security Labor Shortage and International Business Risk* (pp. 1–18). IGI Global. https://doi.org/10.4018/978-1-5225-5927-6.ch001

Halkias, D., Neubert, M., Thurman, P. W., & Harkiolakis, N. (2022). *The Multiple case study design: Methodology and application for management education*. Routledge.

Har, L. L., Rashid, U. K., Te Chuan, L., Sen, S. C., & Xia, L. Y. (2022). Revolution of retail industry: from perspective of retail 1.0 to 4.0. *Procedia Computer Science*, *200*, 1615–1625. https://doi.org/10.1016/j.procs.2022.01.362

Hayes, P., & Kelly, S. (2018). Distributed morality, privacy, and social media in natural disaster response. *Technology in Society*, *54*, 155-167. https://doi.org/10.1016/j.techsoc.2018.05.003

Hiscox. (2019). Cyber readiness report 2019. Chesney House. https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

Hiscox. (2021). Hiscox cyber readiness report 2021: Don't let cyber be a game of chance. Chesney House. https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2021.pdf

Hourigan, R. M., & Edgar, S. N. (2020). 7.1. The Foundations of Phenomenology: Epistemology, Methodology, and Analysis. *Approaches to Qualitative Research: An Oxford Handbook of Qualitative Research in American Music Education, Volume 1*, 110.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, 3171-3189. https://doi.org/10.1007/s13369-019-04319-2

Imtiaz, N., Thorn, S., & Williams, L. (2021, October). A comparative study of vulnerability reporting by software composition analysis tools. In *Proceedings of the 15th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)* (pp. 1–11). https://doi.org/10.1145/3475716.3475769

Jackson, M. C. (2019). *Critical systems thinking and the management of complexity*. John Wiley & Sons.

Jahankhani, H., Meda, L. N., & Samadi, M. (2022). Cybersecurity challenges in small and medium enterprise (SMEs). In *Blockchain and Other Emerging Technologies for Digital Business Strategies* (pp. 1–19). Springer, Cham. https://doi.org/10.1007/978-3-030-98225-6_1

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, *84*(1), 7120. https://doi.org/10.5688/ajpe7120

Kakucha, W., & Buya, I. (2018). Information system security mechanisms in financial management. *Journal of Information and Technology*, *2*(1). https://stratfordjournals.org/journals/index.php/Journal-of-Information-and-Techn/article/view/115

Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. *IEEE Access*, *9*, 37855-37865. https://ieeexplore.ieee.org/abstract/document/9366688

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kantheti, S. C., & Manne, R. (2022). Performance and evaluation of firewalls and security. In *An Interdisciplinary Approach to Modern Network Security* (pp. 69–87). CRC Press.

Katina, P. F., & Keating, C. B. (2018). Cyber-physical systems governance: A framework for (meta)xybersecurity design. In: Masys, A. (eds) *Security by Design. Advanced Sciences and Technologies for Security Applications.* Springer, Cham. https://doi.org/10.1007/978-3-319-78021-4_7

Kaushik, K., Tayal, S., Bhardwaj, A., & Kumar, M. (Eds.). (2021). *Advanced Smart Computing Technologies in Cybersecurity and Forensics*. CRC Press.

Kazdin, A. E. (2021). Single-case experimental designs: Characteristics, changes, and challenges. *Journal of the Experimental Analysis of Behavior*, *115*(1), 56-85. https://doi.org/10.1002/jeab.638

Kekeya, J. (2021). Qualitative case study research design: The commonalities and differences between collective, intrinsic and instrumental case studies. *Contemporary PNG Studies*, *36*, 28-37.

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*, *10*(10), 1168. https://doi.org/10.3390/electronics10101168

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. *South African Journal of Information Management, 23*(1). https://doi.org/10.36227/techrxiv.12278792.v1

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyberattacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident; Analysis and Prevention*, *148*, Article 105837. https://doi.org/10.1016/j.aap.2020.105837

Khatoon, S., Asif, A., Hasan, M. M., & Alshamari, M. (2022). Social media-based intelligence for disaster response and management in smart cities. In *Artificial Intelligence, Machine Learning, and Optimization Tools for Smart Cities: Designing for Sustainability* (pp. 211-235). Cham: Springer International Publishing.

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher*, *42*(8), 846-854. https://doi.org/10.1080/0142159X.2020.1755030

Kilgour, L. (2020). The ethics of aesthetics: Stigma, information, and the politics of electronic ankle monitor design. *The Information Society*, *36*(3), 131–146. https://doi.org/10.1080/01972243.2020.1737606

Kim, S., Yoon, S., Narantuya, J., & Lim, H. (2020). Secure collecting, optimizing, and deploying of firewall rules in software-defined networks. *IEEE Access*, *8*, 15166-15177. https://ieeexplore.ieee.org/abstract/document/8962096

Kipper, L. M., Iepsen, S., Dal Forno, A. J., Frozza, R., Furstenau, L., Agnes, J., & Cossul, D. (2021). Scientific mapping to identify competencies required by industry 4.0. *Technology in Society, 64*, 101454–101463. https://doi.org/10.1016/j.techsoc.2020.101454

Kitteringham, G., & Fennelly, L. J. (2020). Environmental crime control, in *Handbook of Loss Prevention and Crime Prevention (6th Ed.).* Elsevier.

Kizza, J. M. (2020). Cyber crimes and hackers. *Guide to Computer Network Security,* 105–131. https://doi.org/10.1007/978-3-030-38141-7_5

Kuhn, T. (1970). *The structure of scientific revolutions*. Chicago, IL: University of Chicago Press.

Kusumastuti, S. A., Blythe, J., Rosoff, H., & John, R. S. (2020). Behavioral determinants of target shifting and deterrence in an analog cyberattack game. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *40*(3), 476–493. https://doi.org/10.1111/risa.13402

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyberattacks during the pandemic. *Computers & Security*, *p. 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Lee, Y. Y., & Falahat, M. (2019). The impact of digitalization and resources on gaining competitive advantage in international markets: Mediating role of marketing, innovation and learning capabilities. *Technology Innovation Management Review*, *9*(11). https://doi.org/10.22215/timreview/1281

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy, 6*(2), 118–136. https://doi.org/10.1080/23738871.2021.1880609

Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using Leximancer for qualitative data analysis triangulation. *The Qualitative Report, 25*(3), 604–614.

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA Publications and Communications Board task force report. *American Psychologist*, *73*(1), 26–38. https://doi.org/10.1037/amp000015

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry, 103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

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

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyberattacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, Y., Tong, Y., & Giua, A. (2020). Detection and prevention of cyberattacks in networked control systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

Liamputtong, P. (2019). *Handbook of research methods in health social sciences.* Springer Singapore. https://philpapers.org/rec/LIAHOR

Lindgren, B. M., Lundman, B., & Graneheim, U. H. (2020). Abstraction and interpretation during the qualitative content analysis process. *International Journal of Nursing Studies, 108*, Article 103632. https://doi.org/10.1016/j.ijnurstu.2020.103632

Liu, T., Wang, C., Wang, Y., Huang, L., Li, J., Xie, F., Zhang, J., & Hu, J. (2020). Impacts of model resolution on predictions of air quality and associated health exposure in Nanjing, China. *Chemosphere, 249*, 126515. https://doi.org/10.1016/j.chemosphere.2020.126515

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*, *2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

Logeshwaran, J., Ramesh, G., & Aravindarajan, V. (2023). A secured database monitoring method to improve data backup and recovery operations in cloud computing. *BOHR International Journal of Computer Science*, *2*(1), 1-7.

Low, J. (2019). A pragmatic definition of the concept of theoretical saturation. *Sociological Focus*, *52*(2), 131-139. https://www.tandfonline.com/doi/abs/10.1080/00380237.2018.1544514

Lu, X., Niyato, D., Privault, N., Jiang, H., & Wang, S. S. (2018, May). A cyber insurance approach to manage physical layer secrecy for massive MIMO cellular networks. *2018 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2018.8422833

Madhuri, P., & Prabhu, E. (2023). Data protection using scrambling technique. In *Inventive computation and information technologies: Proceedings of ICICIT 2022* (pp. 811-822). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-7402-1_58

McGrath, R., Bowen-Salter, H., Milanese, E., & Pearce, P. (2021). Developing a Collaborative AutoNetnographic approach to researching doctoral students' online experiences. In *Qualitative and Digital Research in Times of Crisis: Methods, Reflexivity, and Ethics* (pp. 113-128). Policy Press. https://doi.org/10.51952/9781447363828.ch007

Merriam, S. B., & Grenier, R. S. (Eds.). (2019). Qualitative research in practice: Examples for discussion and analysis. John Wiley & Sons.

Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. Mesopotamian Journal of Cybersecurity, 2023, 1-6.

Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyberattacks on industrial control systems.

International Journal of Critical Infrastructure Protection, *35*, 100464. https://www.sciencedirect.com/science/article/abs/pii/S1874548221000524

Mohajan, H. K. (2020). Quantitative research: A successful investigation in natural and social sciences. *Journal of Economic Development, Environment and People*, *9*(4), 50-79.

Mohammad, R. M. A. (2020). A lifelong spam emails classification model. *Applied Computing and Informatics, ahead-of-print(ahead-of-print)*. https://doi.org/10.1016/j.aci.2020.01.002

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*(4), 1–9. https://doi.org/10.1007/s11920-021-01228-w

Moustakas, C. (1994). *Phenomenological research methods.* Sage.

Muheidat, F., Tawalbeh, M., Quwaider, M., & Saldamli, G. (2020, October). Predicting and preventing cyberattacks during covid-19 time using data analysis and proposed secure iot layered model. In *2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)* (pp. 113–118). IEEE. https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1050315

Müller, J. M. (2019). Business model innovation in small-and medium-sized enterprises: Strategies for industry 4.0 providers and users. *Journal of Manufacturing Technology Management*, *30*(8), 1127-1142. https://doi.org/10.1108/JMTM-01-2018-0008

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. U.S. Department of Health and Human Services. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

Natow, R. S. (2020). The use of triangulation in qualitative studies employing elite interviews. *Qualitative Research*, *20*(2), 160-173. https://doi.org/10.1177/1468794119830077

Ncubukezi, T. (2023). Risk likelihood of planned and unplanned cyberattacks in small business sectors: A cybersecurity concern. *International Conference on Cyber Warfare and Security*, *18*(1), 279–290. https://doi.org/10.34190/iccws.18.1.1084

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020, December). A review of the current cyber hygiene in small and medium-sized businesses. In *2020 15th International Conference for internet Technology and Secured Transactions (ICITST)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/9351339

Nobles, C., & Burrell, D. (2018, March). Using cybersecurity communities of practice (CoP) to support small and medium businesses. In *ICIE 2018 6th International Conference on Innovation and Entrepreneurship: ICIE 2018* (p. 333). Academic Conferences and publishing limited. http://toc.proceedings.com/38825webtoc.pdf

Nöth, W. (2021). System, sign, information, and communication in cyber semiotics, systems theory, and peirce. In *Introduction to Cybersemiotics: A*

Transdisciplinary Perspective. Springer, Cham. https://doi.org/10.1007/978-3-030-52746-4_4

Okereafor, K., & Adelaiye, O. (2020). Randomized cyberattack simulation model: A cybersecurity mitigation proposal for post COVID-19 digital era. *International Journal of Recent Engineering Research and Development*, *5*(7), 61–72. https://www.researchgate.net/publication/343318105_Randomized_Cyber_Attack_Simulation_Model_A_Cybersecurity_Mitigation_Proposal_for_Post_COVID-19_Digital_Era

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494. https://doi.org/10.1016/j.cose.2021.102494

Papaspirou, V., Maglaras, L., Ferrag, M. A., Kantzavelou, I., Janicke, H., & Douligeris, C. (2021, July). A novel two-factor honeytoken authentication mechanism. In *2021 International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-7). IEEE. https://ieeexplore.ieee.org/abstract/document/9522319

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2018). Cybercrime is whose responsibility? A case study of an online behavior system in crime. *Global Crime*, *19*(1), 1–21. https://doi.org/10.1080/17440572.2017.1411807

Parker, C., Scott, S., & Geddes, A. (2019). Snowball sampling. *SAGE research methods foundations*. https://eprints.glos.ac.uk/6781/

Patel, S., Patel, D., & Nazir, S. (2020). *Cloud-based autonomic computing framework for securing SCADA systems.* IGI Global. https://doi.org/10.4018/978-1-7998-3038-2

Patterson, A. (2020). The ongoing issue of cyber insecurity why cyber insurance should be mandatory for consumer companies. *Florida State UL Review*, *48*, 841. https://heinonline.org/HOL/LandingPage?handle=hein.journals/flsulr48&div=26&id=&page=

Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080.

Paxton, A. (2020). The Belmont Report in the age of big data: Ethics at the intersection of psychological science and data science. In S. E. Woo, L. Tay, & R. W. Proctor (Eds.), *Big data in psychological research* (pp. 347–372). American Psychological Association. https://doi.org/10.1037/0000193-016

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 319-338). Accessed from: https://www.usenix.org/conference/soups2019/presentation/pearman

Permana, G. R., Trowbridge, T. E., & Sherborne, B. (2022). Ransomware mitigation: An analytical investigation into the effects and trends of ransomware attacks on global business. Preprint from PsyArXiv. https://doi.org/10.31234/osf.io/ayc2d

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific*

Research and Management, 9 (12), 669–710. https://hal.science/hal-03509116/document

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371-390. https://link.springer.com/article/10.1007/s10111-021-00683-y

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *internet Technology Letters, 4*(2). https://doi.org/10.1002/itl2.247

Prosek, E. A., & Gibson, D. M. (2021). Promoting rigorous research by examining lived experiences: A review of four qualitative traditions. *Journal of Counseling & Development*, *99*(2), 167-177. https://doi.org/10.1002/jcad.12364

Puławska, K., Strzelczyk, W., & Orzechowski, A. (2022). Cyber insurance and information sharing as prevention from cyberattacks – pilot study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4260821

Purkait, S., & Damle, M. (2023, March). Cyber security and frameworks: A study of cyberattacks and methods of prevention of cyberattacks. In *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 1310-1315). IEEE. https://ieeexplore.ieee.org/abstract/document/10104823

Quintão, C., Andrade, P., & Almeida, F. (2020). How to Improve the Validity and Reliability of a Case Study Approach?. *Journal of Interdisciplinary Studies in Education*, *9*(2), 264-275. https://doi.org/10.32674/jise.v9i2.2026

Raineri, E. M., & Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. *Journal of Applied Business and Economics, 22*(12). https://doi.org/10.33423/jabe.v22i12.3876

Ranta, V., Aarikka-Stenroos, L., & Väisänen, J. M. (2021). Digital technologies catalyzing business model innovation for circular economy—Multiple case study. *Resources, Conservation and Recycling, 164,* https://doi.org/10.1016/j.resconrec.2020.105155

Raskind, I. G., Shelton, R. C., Comeau, D. L., Cooper, H. L., Griffith, D. M., & Kegler, M. C. (2019). A review of qualitative data analysis practices in health education and health behavior research. *Health Education & Behavior, 46*(1), 32–39. https://journals.sagepub.com/doi/pdf/10.1177/1090198118795019

Reimsbach, D., & Braam, G. (2022). Creating social and environmental value through integrated thinking: International evidence, *Business Strategy and the Environment,* 3131, 32(1), 304-320. https://doi.org/10.1002/bse.3131

Rodriguez, J. C. (2019). Posture of the local government in Puerto Ricority measures small retail businesses. Walden University. https://scholarworks.waldenu.edu/dissertations?utm_source=scholarworks.waldenu.edu%2Fdissertations%2F6370&utm_medium=PDF&utm_campaign=PDFCoverPages

Rosati, P., Deeney, P., Cummins, M., Van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance*, *pp. 47*, 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007

Rose, J., & Johnson, C. W. (2020). Contextualizing reliability and validity in qualitative research: Toward more rigorous and trustworthy qualitative social science in leisure research. *Journal of Leisure Research, 51*(4), 432–451. https://doi.org/10.1080/00222216.2020.1722042

Ross, P. T., & Bibler Zaidi, N. L. (2019). Limited by our limitations. *Perspectives on Medical Education, 8*(4), 261–264. https://doi.org/10.1007/s40037-019-00530-x

Roth, S. (2019). The open theory and it's enemy: Implicit moralization as an epistemological obstacle for general systems theory. *Systems Research and Behavioral Science*, *36*(3), 281–288. https://doi.org/10.1002/sres.2590

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

Rowlands, J. (2021). Interviewee transcript review as a tool to improve data quality and participant confidence in sensitive research. *International Journal of Qualitative Methods*, *20*, Article 16094069211066170. https://journals.sagepub.com/doi/pdf/10.1177/16094069211066170

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Saldaña, J. (2021). *The coding manual for qualitative researchers*. Oxford. https://doi.org/10.1093/oxfordhb/9780199811755.013.001

Sanders, P., Bronk, C., & Bazilian, M. D. (2022). Critical energy infrastructure and the evolution of cybersecurity. *The Electricity Journal*, *35*(10), 107224. https://doi.org/10.1016/j.tej.2022.107224

Satterfield, K., Mancuso, V. F., Strang, A., Greenlee, E., Miller, B., & Funke, G. J. (2018). When actions speak louder than words: Using changes in operator behavior and system efficiency measures to detect the presence of a cyberattack. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62*(1), 270–271. https://doi.org/10.1177/1541931218621062

Saura, J. R., Palacios-Marqués, D., & Iturricha-Fernández, A. (2021). Ethical design in social media: Assessing the main performance measurements of user online behavior modification. *Journal of Business Research, 129*, 271–281. https://doi.org/10.1016/j.jbusres.2021.03.001

Schaupp, L. C., & Bélanger, F. (2014). The value of social media for small businesses. *Journal of Information Systems, 28*(1), 187-207. https://doi.org/10.2308/isys-50674

Sembada, A. Y., & Koay, K. Y. (2021). How perceived behavioral control affects trust to purchase in social media stores. *Journal of Business Research, 130*, 574–582. https://doi.org/10.1016/j.jbusres.2019.09.028

Shaverdian, P. (2019). Start with trust: utilizing blockchain to resolve the third-party data breach problem. *UCLA Law Review*, *66*, 1242. https://heinonline.org/HOL/LandingPage?handle=hein.journals/uclalr66&div=35&id=&page=

Shoenberger, N. (2021). Applying routine activity theory: A case study of the Sonya Farak drug scandal. *Open Journal of Social Sciences*, 9, 118–129. doi:https://doi.org/10.4236/jss.2021.910009

Siahaan, A. P. U., & Nasution, M. D. T. P. (2018). The phenomenon of cyber-crime and fraud victimization in online shop. *International Journal of Civil Engineering and Technology, 9*(6), 1583–1592.

Small, A., Owen, A., & Paavola, J. (2021). Organizational use of ecosystem service approaches: A critique from a systems theory perspective. *Business Strategy and the Environment, 13*(1). https://doi.org/10.1002/bse.2887

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies, *Journal of Cybersecurity*, *7*(1), tyab019. https://doi.org/10.1093/cybsec/tyab019

Sombultawee, K., & Wattanatorn, W. (2022). Management of social selling and B2B customer-brand engagement: is direct selling on social media good for your brand and relationships? *Electronic Commerce Research and Applications*, *54*, 101167–101179. https://doi.org/10.1016/j.elerap.2022.101167

Sophy, J. (2021). *43 percent of cyberattacks target small business*. Technology Trends. https://smallbiztrends.com/2016/04/cyberattacks-target-small-business.html?utm_content=cmp-true

Stahl, N. A., & King, J. R. (2020). Expanding approaches for research: Understanding and using trustworthiness in qualitative research. *Journal of Developmental Education*, *44*(1), 26-28. https://www.jstor.org/stable/45381095

Staller, K. M. (2021). Big enough? Sampling in qualitative inquiry. *Qualitative Social Work*, *20*(4), 897-904. https://journals.sagepub.com/doi/pdf/10.1177/14733250211024516

Stewart, H. (2022). Digital transformation security challenges. *Journal of Computer Information Systems*, 1–18. https://doi.org/10.1080/08874417.2022.2115953

Stratton, S. J. (2021). Population research: convenience sampling strategies. *Prehospital and disaster Medicine*, *36*(4), 373-374. https://doi.org/10.1017/S1049023X21000649

Sulaiman, N., Hamdan, A., & Al Sartawi, A. (2022). The influence of cybersecurity on the firms' financial performance. In: Hamdan, A., Harraf, A., Arora, P., Alareeni, B., Khamis Hamdan, R. (eds) *Future of Organizations and Work After the 4th Industrial Revolution. Studies in Computational Intelligence, vol 1037.* Springer, Cham. https://doi.org/10.1007/978-3-030-99000-8_25

Susanto, H., Fang Yie, L., Mohiddin, F., Rahman Setiawan, A. A., Haghi, P. K., & Setiana, D. (2021). Revealing social media phenomenon in time of COVID-19 pandemic for boosting start-up businesses through digital ecosystem. *Applied System Innovation, 4*(1), 6. https://doi.org/10.3390/asi4010006

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A narrative review of cybersecurity implications for Australian small businesses. In *arXiv [cs.CR]*. http://arxiv.org/abs/2109.00733

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660–671. https://doi.org/10.1016/j.future.2019.03.042

Temel, S., & Durst, S. (2020). Knowledge risk prevention strategies for handling new technological innovations in small businesses. *VINE Journal of Information and Knowledge Management Systems*, *4*(51), 655–673. https://doi.org/10.1108/VJIKMS-10-2019-0155

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative Nursing-Quarterly Scientific, Online Official Journal of GORNA, 7*(3), 155–163. https://doi.org/10.5281/zenodo.2552022

Thomson, L., Kamalaldin, A., Sjödin, D., & Parida, V. (2022). A maturity framework for autonomous solutions in manufacturing firms: The interplay of technology, ecosystem, and business model. *International Entrepreneur Management Journal*, *18*, 125–152. https://doi.org/10.1007/s11365-020-00717-3

Timans, R., Wouters, P., & Heilbron, J. (2019). Mixed methods research: what it is and what it could be. *Theory and Society, 48,* 193–216. https://doi.org/10.1007/s11186-019-09345-5

Tura, N., Keränen, J., & Patala, S. (2019). The darker side of sustainability: Tensions from sustainable business practices in business networks. *Industrial Marketing Management, 77*, 221-231. https://doi.org/10.1016/j.indmarman.2018.09.002

Udofot, M., & Topchyan, R. (2020). Factors related to small business cyberattack protection in the United States. *International Journal of Cyber-Security and Digital Forensics*, *9*(1), 12–25. https://doi.org/10.17781/p002644

Unger, A. (2021). Susceptibility and response of small business to cyberattacks (Doctoral dissertation, Utica College). Proquest: 28495687. https://www.proquest.com/openview/c6d0bf13fcf0ca37dae88f5ea6d5f2a8/1?pq-origsite=gscholar&cbl=18750&diss=y

U.S. Small Business Administration. (2022). Small Business Size Standards: Wholesale Trade and Retail Trade. *Federal Register.* https://www.federalregister.gov/documents/2022/06/14/2022-12512/small-business-size-standards-wholesale-trade-and-retail-trade

Van Assche, K., Verschraegen, G., Valentinov, V., & Gruezmacher, M. (2019). The social, the ecological, and the adaptive: Von Bertalanffy's general systems theory and the adaptive governance of social-ecological systems. *Systems Research and Behavioral Science, 36*(3), 308–321. https://doi.org/10.1002/sres.2587

Vanderstraeten, R. (2019). Systems everywhere? *Systems Research and behavioral Science*, *36*(3), 255–262. https://doi.org/10.1002/sres.2596

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

von Bertalanffy, L. (1968). *General systems theory: Foundations, development, application* (Rev. ed.). George Braziller. https://repository.vnu.edu.vn/handle/VNU_123/90608%20

von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal, 15*(4), 407–426. https://doi.org/10.5465/255139

Vu, T. T. N. (2021). Understanding validity and reliability from qualitative and quantitative research traditions. *VNU Journal of Foreign Studies*, *37*(3). https://doi.org/10.25073/2525-2445/vnufs.4672

Wang, Z., Li, M., Lu, J., & Cheng, X. (2022). Business innovation based on artificial intelligence and blockchain technology. *Information Process. Management*, *59*,102759. https://doi.org/10.1016/j.ipm.2021.102759

Ward, P. (2022). Community college cybersecurity programs: A proposed framework. In *Proceedings of the EDSIG Conference ISSN*, *2473*, 4901. https://proc.iscap.info/2022/pdf/5824.pdf

White, C. (2018). Challenging traditional research assumptions: Critical qualitative research in social/global education. *Internationalizing Education* (pp. 1–8). Brill. https://doi.org/10.1163/9789004364622_001

Wibowo, A., Chen, S. C., Wiangin, U., Ma, Y., & Ruangkanjanases, A. (2020). Customer behavior as an outcome of social media marketing: The role of social media marketing activity and customer experience. *Sustainability*, *13*(1), 189. https://doi.org/10.3390/su13010189

Wilbanks, L. R. (2020). Cyber risks in social media. In G. Meiselwitz (Ed.), *Social computing and social media.* Design, ethics, user behavior, and social network analysis (pp. 393–406). Springer. https://doi.org/10.1007/978-3-030-49570-1_27

Wood, L. M., Sebar, B., & Vecchio, N. (2020). Application of rigour and credibility in qualitative document analysis: Lessons learnt from a case study. *The Qualitative*

Report, *25*(2), 456-470. Accessed from: https://research-repository.griffith.edu.au/handle/10072/394518

Wutich, A., & Brewis, A. (2019). Data collection in cross-cultural ethnographic research. *Field Methods*, *31*(2), 181-189. https://doi.org/10.1177/1525822X19837397

Yaokumah, W., Rajarajan, M., Abdulai, J. D., Wiafe, I., & Katsriku, F. A. (Eds.). (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance*. IGI Global.

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

Yu, S. (2020). Crime hidden in email spam. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 851–863). IGI Global. https://www.igi-global.com/book/encyclopedia-criminal-activities-deep-web/223181

Zenker, S., & Kock, F. (2020). The coronavirus pandemic–A critical discussion of a tourism research agenda. *Tourism Management*, *81*, 104164–104168. https://doi.org/10.1016/j.tourman.2020.104164

Zhu, Z. (2021). Paradigm, specialty, pragmatism: Kuhn’s legacy to methodological pluralism. *Journal of the International Society for the Systems Sciences*, *65*(1), 895–912. https://doi.org/10.1002/sres.2881

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile books.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study.

Journal of Computer Information Systems, *62*(1), 82-97.

https://doi.org/10.1080/08874417.2020.1712269

Appendix: Interview Protocol

Date of Interview: _____________

Respondent Number: __________

1. Introduce self to the participant

Thank you for participating in this study and your willingness to complete the interview process. My name is Chris Royal and I'm a student at Walden University conducting research on social media cyberattacks on small retail businesses as part of my dissertation project.

2. Introduce the research question, the purpose of the study and answer any initial questions the participant may have.

The purpose of my study is to identify and explore strategies some U.S. retail leaders use to deter social media cyberattacks. The research question I'm trying to address is: What strategies do some leaders of U. S. small retail businesses use to deter social media cyberattacks? Do you have any initial questions before we get started?

3. Thank the participant for their participation in the study.

Thank you again for agreeing to participate in my study.

4. Review the informed consent form and answer any questions the participant may have.

Before we continue, I need to verify that you have signed the consent form and understand the ethical standards for this interview. All personal information will be stored electronically and may only be accessed to me via a password. Raw data, such as field notes, will be kept locked in a file cabinet only accessible to myself. When the information from the interview is published in the final study, participant confidentiality will remain. All transcripts and recordings of the interview will be kept private on a password-protected computer accessible to myself only. Do you have any questions about the consent form or any of the measures taken to preserve your confidentiality?

5. Provide the participant with a copy of the informed consent form for their personal records and review.

Here's a copy of the informed consent form for your personal records and review.

6. Begin recording the interview.

Do I have your permission to begin recording the interview now?

7. Introduce the participant using their respondent number, the date and time of the interview.

During this interview, I'm going to refer to you as Participant (Insert participant number). Today's date is (insert today's date) and the time of the interview is (Insert Today's time).

8. Start the interview using the interview questions.

1. What has been your experience with social media cyberattacks?
2. What strategies do you use to protect your business from cyberattacks?
3. What is your risk assessment process for cyber security?
4. What risk management strategies do you use to identify and evaluate cyberattack risks?
5. Please describe how you respond to cyberattacks.
6. What systems and processes do you use to protect your business from cyberattacks?

7. What are the important systematic interdependencies and feedback loops that impact the quality of your cyber-defense tactics against social media cyberattacks?
8. What employee training strategies do you use for security procedures with electronic devices?
9. What steps would you advise someone in your position to follow if a cyberattack threatened their small retail business?
10. What is your cyberattack contingency plan?
11. Before we conclude the interview, what additional information about cybersecurity strategies would you like to share?

9. Ask any follow-up questions.

10. End the interview and stop the recording. Explain to the participant of the member checking and transcription review process.

We have reached the end of this interview. Thank you for your participation in this study and sharing your personal experiences with me. I appreciate your transparency and honesty in each of your responses. Do you have any questions about the interview or the research process?

As a reminder, I will take the audio from these recordings and transcribe them verbatim. I will be emailing you a copy of the interview transcript. It would be great if you can review the transcript and make sure that you’re comfortable with all of the responses. If you’d like any changes to be made to the transcript so that it more accurately reflects your thoughts and ideas, please let me know. That’s an important part of the research process.

11. Thank the participant for the participation in the study.

Thank you again for participating in my study. You can contact me at any time if you have any questions or concerns.