Docusign Envelope ID: 745CBD6E-5B02-88AE-81CA-3630B31DDBB8

Marywood
UNIVERSITY

College of Professional Studies

The PhD Program in Strategic Leadership and Administrative Studies

Cybersecurity Strategies for Small Businesses in the Post-COVID-19 Era: A Qualitative Study of Risk, Threats, and Resilience

By

Abinet G. Kidane, DBA, MS, MPP

Submitted in Partial Fulfillment of the Requirements for the Degree
of Ph.D. in Strategic Leadership and Administrative Studies

Position	Name	Signature
Chair, Dissertation Committee	Alan Levine, Ph.D.	Signed by: F8AE2BC776A14D3...
Committee Member	Loreen Powell, Ph.D.	Signed by: 8115E47A52CD455...
Committee Member	Stanley Kania, Ph.D.	Signed by: BECDCE633560477...
Reader	Amy Washo, Ph.D.	DocuSigned by: 176A70F9A9B8489...
Reader	Prof Haileleul Woldemariam	Signed by: 13EC819C4121442...

Approval Date: August 11, 2026

© 2026 Abinet G. Kidane. All rights reserved.

Abstract

Small businesses face growing cybersecurity risks in the post- coronavirus disease 2019 (COVID-19) environment due to rapid digital transformation, remote work, cloud adoption, and increased reliance on interconnected systems. Limited budgets, lack of in-house expertise, and staffing constraints often make these organizations vulnerable to phishing, ransomware, and emerging artificial intelligence (AI)-enabled threats. The purpose of this qualitative study was to explore cybersecurity strategies used by small business leaders to protect their organizations from cyberattacks in the post-COVID-19 era. The study was guided by Transformational Leadership Theory (TLT), the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and the Enterprise Risk Management (ERM) framework. Data was collected through semi-structured interviews with business leaders, and thematic analysis was subsequently employed to identify recurring patterns across participant responses. Findings revealed that cybersecurity has become a core business imperative rather than solely an information technology (IT) issue. Key themes included the importance of foundational controls such as multi-factor authentication (MFA), tested backups, endpoint protection, employee training, written policies, and incident response planning. Participants also emphasized leadership commitment, security culture, cyber insurance, and the need to address resource limitations. AI-driven threats, deepfakes, and automated attacks were identified as major emerging concerns. The study contributes to positive social change by offering practical, scalable strategies that small business leaders can use to reduce cyber risk, protect customer data, sustain operations, and improve resilience. Recommendations include prioritizing basic controls, fostering employee awareness, leveraging external expertise, and embedding cybersecurity into overall business strategy.

Keywords: cybersecurity, small business, post-COVID-19, cyberattacks, phishing, ransomware, AI, leadership, NIST, ERM

Dedication

To my sons, Nathy and Eli, this dissertation is dedicated to you.

You have been my reason to reach for dreams that once felt far beyond my grasp. Because of you, I found the courage to pursue goals I might never have attempted on my own and the strength to see every obstacle as an opportunity to grow rather than a reason to give up.

Along this journey, there were missed games, school events, dinners, and countless moments I wish I could have shared more fully. There were also times when I felt exhausted, discouraged, and ready to stop. Yet, through it all, you remained my greatest source of encouragement, joy, and purpose. You are my best friends and among the greatest blessings God has given me, second only to the love, grace, and salvation found in Jesus Christ.

May this work serve as a reminder that meaningful goals often take time, sacrifice, and perseverance, but the journey is worthwhile when you remain committed to what matters most. Trust in yourselves, remain faithful through life's challenges, and do not be discouraged by setbacks. Your determination, resilience, and willingness to keep learning will carry you toward the future God has prepared for you.

Never forget that your dad loves you beyond measure and will always be your biggest supporter—today, tomorrow, and forever.

Acknowledgments

This journey was carried by grace I did not earn. All glory belongs to God — my provision, my strength, and the quiet and not-so-quiet nudges that kept me moving forward. To Him, I owe everything.

To my dissertation chair, Dr. Alan Levine — thank you for your mentorship and steady belief in this work. Your feedback sharpened my thinking, and your regular check-ins kept me grounded and moving toward the finish line.

To my committee, Dr. Loreen Powell and Dr. Stanley Kania — thank you for the thoughtful insight, valuable feedback, and continuous encouragement that strengthened this work in meaningful ways. To my readers, Dr. Amy Washo and Prof. Haileleul Woldemariam — thank you for your time, expertise, and careful review. Prof. Woldemariam, you have been a mentor and friend for over two decades, and your influence on my professional growth has been immeasurable.

To my wife, Mety — you sacrificed just as much as I did to help me achieve this Ph.D., and often more. Your patience, love, and encouragement never wavered, even when mine did. Thank you for believing in this dream as fully invested as I did and for never allowing me to give up on it.

To my parents — your love, wisdom, and support are the foundation this entire journey was built on. You showed up however I needed, without hesitation. I am so grateful you're here to see this finished, and this achievement belongs to you as much as it does to me.

And to the small business leaders across Seattle metropolitan area who generously shared their time and experiences — this research exists because you were willing to talk. Thank you.

Table of Contents

List of Tables

List of Figures

Chapter One

The Problem and Its Setting

Introduction

Digital technology is what powers modern society. While online technology offers many advantages, such as instant communication, cloud computing, and remote work capabilities, it also comes with significant drawbacks, most notably, the rise in cyberattacks. As businesses, governments, and individuals increasingly rely on internet-connected systems, cybercriminals exploit vulnerabilities through tactics like phishing, ransomware, and data breaches. This demonstrates the urgent need for enhanced cybersecurity measures to protect small businesses from the escalating costs and impacts of cybercrime. Sharif and Mohammed (2022) emphasize the urgent need for businesses to invest in strong cybersecurity measures, adopt proactive risk management strategies, and comply with evolving regulatory standards to mitigate financial losses from cyber threats. The cost of cyberattacks on small businesses can be devastating. The study highlights that cybercrime has led to billions of dollars in losses annually, affecting companies of all sizes, with small businesses being particularly vulnerable due to limited cybersecurity resources. In fact, a cyberattack can cripple a small business's ability to operate, leading to both immediate and long-term financial damage.

One contributing factor to the increase in cyberattacks on small businesses could be their inadequate cybersecurity, often resulting from limited financial resources, outdated equipment, and a shortage of experienced personnel. (Ncubukezi, 2023; El-Hajj & Mirza, 2024; Chagadama et al., 2022) Small businesses often operate with limited budgets, which makes it challenging for them to invest in comprehensive cybersecurity systems and tools. Furthermore, many small businesses may not have the technical expertise or the trained staff

needed to implement and maintain effective security measures. As a result, their networks, systems, and data become more vulnerable to cyber threats such as phishing, ransomware, and data breaches can exploit the existing security gaps. This shortage of resources makes it harder for small businesses to adequately defend themselves against the growing number and complexity of cyberattacks. Another reason could be the lack of awareness and training about cyber threats.

Another study by Thompson (2023) demonstrated a clear and direct correlation between heightened cybersecurity risks and several key vulnerabilities commonly found in small businesses. A multiple regression analysis was conducted using a sample of 252 minority-owned small businesses. The research highlighted that limited financial and human resources often prevent these businesses from implementing robust security measures. The results indicated that all predictor variables were statistically significant in assessing cybersecurity risk. Additionally, a widespread lack of cybersecurity awareness among employees leaves systems more susceptible to phishing attacks and social engineering tactics. Together, these factors create a fragile cybersecurity posture that significantly increases the likelihood of data breaches and cyberattacks. Consequently, it is essential for these businesses to prioritize cybersecurity by investing in appropriate tools, education, and infrastructure to mitigate potential risks and safeguard their operations.

As large businesses and corporations continue to invest in cybersecurity measures, hackers are increasingly focusing on small and medium-sized businesses (FBI Internet Crime Report, 2023). These smaller businesses face a greater risk of cyberattacks compared to their larger counterparts, primarily because they lack the same resources, such as advanced tools and personnel, to effectively safeguard themselves in today's interconnected environment

(Scarpato, 2022). Cybercriminals will always find a way to steal customer and business data and use it for illegal purposes or monetary gain. Cybercriminals utilize a variety of computer devices and the Internet to initiate attacks from any location worldwide, making it challenging for small businesses to keep up with the constantly changing threats. As a result, it is critical for small business leaders to prioritize cybersecurity and invest in appropriate protection to make them less vulnerable to cyberattacks (Bryan, 2020).

Like large corporations, small businesses have increasingly adopted digital technologies to support remote work, streamline manufacturing processes, and expand online sales. However, many small business leaders have historically underestimated the importance of cybersecurity, often due to limited resources or a perception that they are unlikely targets. As a result, small businesses are now experiencing cyber breaches at a far higher rate than larger enterprises, which typically have more robust cybersecurity infrastructure, dedicated IT staff, and greater awareness of cyber risks (Verizon Data Breach Investigations Report, 2020). As a result, the risk of cyberattacks for small businesses has considerably increased in recent years, already being higher than the risk for large corporations. A recent report by Cybersecurity Ventures (2022) highlights that global cybercrime damages, including data breaches, are expected to cost the world $10.5 trillion annually by 2025, up from $3 trillion in 2015. This trend represents a significant increase in the frequency and severity of cyberattacks, particularly targeting small businesses.

Although their expanded computer networks have introduced new vulnerabilities to phishing and ransomware attacks, small business leaders have not committed to major cybersecurity spending (Ponemon Institute, 2021). As noted in the ASD Cyber Threat Report (July 2022–June 2023), the increased sophistication of cyber threats, such as phishing and

ransomware, continues to impact organizations, with many small businesses failing to allocate sufficient resources toward cybersecurity protection. Additionally, the Office of the Australian Information Commissioner's (OAIC) Notifiable Data Breaches Report (January to June 2023) also highlights the failure of businesses to allocate sufficient resources for cybersecurity, despite the alarming increase in data breach incidents (OAIC, 2023).

Furthermore, a study by Chidukwani et al. (2022) emphasizes the ongoing reluctance of small business leaders to prioritize cybersecurity spending, which leaves them particularly vulnerable to a wide range of threats, including phishing, ransomware, and data breaches. The researchers conducted a comprehensive literature review to assess the cybersecurity preparedness of small-to-medium businesses (SMBs), focusing on their awareness of cyber risks, the implementation of the NIST Cybersecurity Framework (CSF), and the resources they utilize for guidance. This method enabled them to synthesize findings from various empirical studies and industry reports, offering a holistic view of the current cybersecurity challenges faced by SMBs.

The study also found that while most small businesses recognize the importance of cybersecurity, many still lack the financial resources, technical expertise, and structured strategies needed to implement effective protections. Additionally, SMBs often narrowly focused their cybersecurity efforts and failed to align them with the full spectrum of NIST CSF recommendations. Key challenges cited included insufficient awareness, competing operational priorities, and a general underestimation of cyber risks. The authors conclude with a call for more targeted research, policy development, and educational outreach to better support SMBs in building resilient cybersecurity infrastructures.

A thorough review of existing literature reveals a significant gap in academic research addressing the *true* impact of the COVID-19 pandemic on cybersecurity, particularly within the context of the Western United States. Most studies tend to focus on global or national trends, without offering a deep exploration of how regional variations—such as those found in the Seattle metropolitan area—are uniquely affected. For instance, a study by Chidukwani et al. (2022) focuses on Western Australia, which may limit the generalizability of its findings to small businesses in other regions with different economic and regulatory environments. pandemic. Furthermore, many researchers base their analyses on secondary data, which excludes responses from small business leaders. Research on cyberattacks in a post-pandemic era for small businesses is limited and there is a significant need for more research into the effectiveness of current cybersecurity practices, particularly regarding risk assessment and mitigation for small businesses (Adriko & Nurse, 2024). Government intervention, including regulations and financial support, plays an essential role in helping small businesses improve their cybersecurity defenses. By filling a gap in literature, this study will add to the body of knowledge required to address this problem. This study will highlight the necessity of information security for small businesses, and failing to protect organizational data can result in a data breach that may severely impact the company. The information gathered in this research can act as a valuable resource for small business leaders, drawing attention to the importance of safeguarding sensitive data within their businesses.

The problem in this study is that small business leaders lack effective cybersecurity strategies necessary to protect their businesses from cyberattacks in the post-COVID-19 era. (Ali et al, 2022) Research highlights that despite the growing threats posed by cyberattacks, particularly after the pandemic, many small business leaders have been slow to implement

robust cybersecurity measures. The SBA report (2023) emphasizes the importance of cybersecurity for small businesses and the gaps in their preparedness against cyber threats. Although it is impossible to completely protect against cyber threats, businesses should try to implement the most effective cybersecurity strategies and procedures to ensure that all client and company data are secure. Small business leaders do not always take cybersecurity risks seriously.

There are still common cybersecurity misconceptions that small business leaders must address while developing an effective security plan in their organizations (Wieder & Jansen, 2022). Many small business leaders hold the belief that their companies are "too small" to be vulnerable to a potential data breach. Previous studies provided strong support for the claim that small businesses often dismiss the risk of cyberattacks, leading to insufficient cybersecurity measures. Verizon's (2023) Data Breach Investigations Report highlights how small businesses frequently underestimate their attractiveness to cybercriminals, despite being primary targets for attacks. McAlaney (2022) discusses how small business leaders often believe they are not viable targets, leading to a lack of proactive cybersecurity measures. The National Cyber Security Alliance (2022) report finds that many small business owners assume their businesses are too insignificant for cybercriminals, which contributes to weak security postures.

Although the COVID-19 pandemic has officially ended, small businesses are now more vulnerable to data breaches than pre-pandemic data breaches (Meng et al., 2023). More cyberattacks become possible due to the increased use of insecure networks and cloud technologies. Small business leaders often fail to recognize the attack on their companies until it's too late (SBA, 2021). Half of small businesses have been hacked, and over 60% of those

have closed. Furthermore, an IBM 2021 survey shows that 52% of small firms experienced a cyberattack in the preceding year. Meanwhile, according to a recent poll conducted by UpCity, a Chicago-based business service provider, only 50% of small firms in the United States have a cybersecurity plan in place for 2022 (UpCity, 2022). This study will explore qualitative data and analyze responses to semi-structured interview questions provided by participants. The information gathered in this study will assist small business leaders in developing better strategies for defending their systems against cyberattacks.

Theoretical Framework

The study applied Transformational Leadership Theory (TLT) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework as part of the Enterprise Risk Management (ERM) framework as the theoretical framework. The ERM framework functions as a communication tool to help identify, assess, respond to, and manage both internal and external risks. Meanwhile, TLT provides a lens to understand how leadership behaviors—such as inspiring a shared vision, fostering innovation, and encouraging employee development—can influence the implementation and effectiveness of cybersecurity practices within small businesses. These frameworks align with the goals of the study and will be integrated into the conceptual framework utilized by small business leaders and information security officers responsible for cybersecurity decision-making. They are essential in protecting business and customer data from cyberattacks.

Transformational Leadership Theory

Transformational Leadership Theory (TLT), developed by Burns (1978) and expanded by Bass (1985), serves as a valuable framework for understanding how small business leaders can effectively address cybersecurity challenges. The theory emphasizes leaders' roles in

inspiring, motivating, and transforming their teams to achieve higher levels of performance. In the context of cybersecurity, transformational leaders help cultivate a strong security culture by promoting a shared vision, encouraging innovation, and fostering ethical behavior. Historically, transformational leadership gained prominence during the 1980s and 2000s, evolving from earlier models such as the Blake and Mouton Grid. The theory focuses on the leader's ability to influence employees to go beyond routine tasks by emphasizing employee development and ethical practices (Antonakis & Day, 2018). It helps employees see how their daily responsibilities align with the organization's broader mission, which fosters deeper engagement and accountability (Wood, 2019).

Transformational leaders (TLs) inspire their followers to fully commit to organizational goals and achieve results that surpass typical expectations. As outlined by Bass (1985), TLs do this by (1) increasing followers' awareness of the significance and worth of specific objectives, (2) encouraging them to put the organization's or team's interests ahead of their own, and (3) appealing to their higher-level needs by presenting an inspiring vision and serving as role models who embody that vision. More precisely, TLs exert idealized influence on their subordinates through their distinctive charisma, leading followers to form a personal connection with them (Bass, 1985). This emotional bond fosters a desire among followers to imitate their leaders, making TLs natural role models. By articulating a compelling and ambitious vision for the team or organization and demonstrating confidence in followers' capacity to reach that vision, TLs inspire and motivate them to exceed normal expectations (Olaniyi et al., 2023).

Figure 1

Transformational Leadership Theory

Figure 1 explains transformational leadership through five interconnected practices that help leaders drive meaningful and lasting change. At the core is the idea that leadership is more than simply managing tasks—it is about inspiring and empowering followers to grow and achieve shared goals. The first practice, *Modeling the Way*, highlights the importance of leaders setting a consistent example through their actions and values, thereby establishing clear standards of excellence that others can follow. *Encouraging the Heart* focuses on the emotional dimension of leadership by recognizing and celebrating team members' contributions, which fosters motivation and a sense of belonging, especially during challenging times. *Inspiring a Shared Vision* is about crafting and communicating an appealing future that unites people under a common purpose, encouraging them to work collectively toward that goal. *Enabling Others to Act* underscores the significance of trust and empowerment, as transformational leaders create environments where team members feel

confident to take initiative, collaborate, and make decisions. Finally, *Challenging the Process* involves questioning traditional approaches and encouraging innovation, experimentation, and learning from setbacks to drive improvement. Together, these five practices form a cohesive framework that enables transformational leaders to bring out the best in their followers and guide organizations through meaningful, positive change.

Small businesses, with limited resources and technical expertise, rely heavily on transformational leaders to shape cybersecurity practices. They embed awareness into everyday operations, engage employees through training and involvement in security initiatives, and promote the adoption of innovative technologies. These leaders also emphasize compliance with cybersecurity regulations and ethical standards, which helps reduce organizational vulnerabilities. This leadership model also informs the development of research questions designed to explore cybersecurity practices in small businesses. Questions might address how leaders communicate cybersecurity goals, motivate employees, support training, allocate resources, and balance innovation with risk management. By grounding research in TLT, scholars can better understand how leadership behavior influences cybersecurity preparedness and resilience in the post-COVID-19 landscape.

Research indicates that companies led by transformational leaders enjoy notable performance benefits. These include up to 20% higher employee retention, 17% greater job satisfaction, and 23% increased workforce productivity (Benmira, 2021). Organizations that align leadership vision with business strategy also experience stronger financial stability and up to 18% higher return on investment (Nugroho et al., 2020). In contrast, a lack of effective leadership—often due to competency gaps—can result in poor performance, financial stress, and diminished investor confidence (Widodo, 2022). Overall, transformational leadership

plays a pivotal role in modern organizational success. It not only drives innovation and employee commitment but also helps organizations navigate challenges and maintain resilience, particularly during periods of change or economic uncertainty.

Cybersecurity Risk Management Framework

A cyber risk management framework assists businesses in protecting critical infrastructure by addressing issues encountered during the development of analytical models, identifying opportunities, and protecting assets (Lee, 2021). Cybersecurity professionals must design models to identify vulnerabilities and propose innovative solutions for their resolution. Enhanced connectivity, digital processing, and remote data storage can increase industrial productivity, quality, and cost. Each framework has its own set of guiding principles and regulations, and businesses may choose to employ different frameworks based on their specific demands and regulatory compliance requirements. While individual risk management frameworks may differ in their specific procedures or terminology, a typical framework will often include the following elements: risk identification, risk assessment, risk evaluation, risk response, risk monitoring and review, communication, and reporting.

While there are other frameworks available, this assessment focuses on the NIST CSF. The NIST CSF is a globally recognized standard for cybersecurity guidelines and best practices for enterprise-scale companies securing critical infrastructure (Toussaint, 2024). The framework is a versatile paradigm for developing an ERM framework for firms that rely on technology, are worried about data privacy, and manage risk linked with the most recent digital workforce trends. Although the framework was originally designed for critical infrastructure organizations and businesses collaborating with U.S. government agencies, it has demonstrated its versatility and applicability across different sectors and various

organizations. By using the framework, organizations are better equipped to manage their cybersecurity risks in a cost-effective manner, maximizing their return on security investment.

NIST is particularly beneficial for firms relying on technology, data privacy, and risk management related to digital workforce trends. Through the implementation of the framework, organizations can efficiently manage their cybersecurity risks, ensuring both compliance and optimal security investment (Toussaint, 2024). Additionally, the NIST framework provides a standardized language, reducing ambiguities in contract terms and agreements. Nonetheless, the absence of prescriptive regulations and formal certification within the NIST CSF may result in certain organizations facing uncertainty and finding it challenging to prove compliance to external stakeholders (Al-Hawamleh, 2024). Table 1 outlines the components of the framework in alignment with ERM, which include risk identification, risk assessment, risk evaluation, risk response, risk monitoring and review, communication, and reporting. This structured process effectively manages cybersecurity risks within small businesses. By aligning these ERM components with the NIST Cybersecurity Framework and guided by the principles of Transformational Leadership Theory, small business leaders can foster a proactive cybersecurity culture that enhances resilience and reduces vulnerability to cyber threats.

Table 1.

NIST CSF functions and classifications

NIST CSF Function	Category
Identify	Asset management; Risk assessment; Governance and compliance; Responsibilities; Risk Management; Procurement / supply chain risk management; Working with external partners; Recruitment
Protect	Identity management and user access control; Awareness and Training; Data Security; Information protection processes and procedures; Encryption; Maintenance; Patch and change management; Protective technology
Detect	Detection process; Security Incident Event Monitoring (SIEM) & anomalies; Security continuous monitoring
Respond	Response planning; Communications management; Forensics and impact analysis; Incident management; Emergency management; Lessons learnt and continuous improvement
Recover	Disaster recovery (DRP); Business continuity management (BCP); Improvements; Communications

Note. Source: NIST (2021)

Conceptual Framework

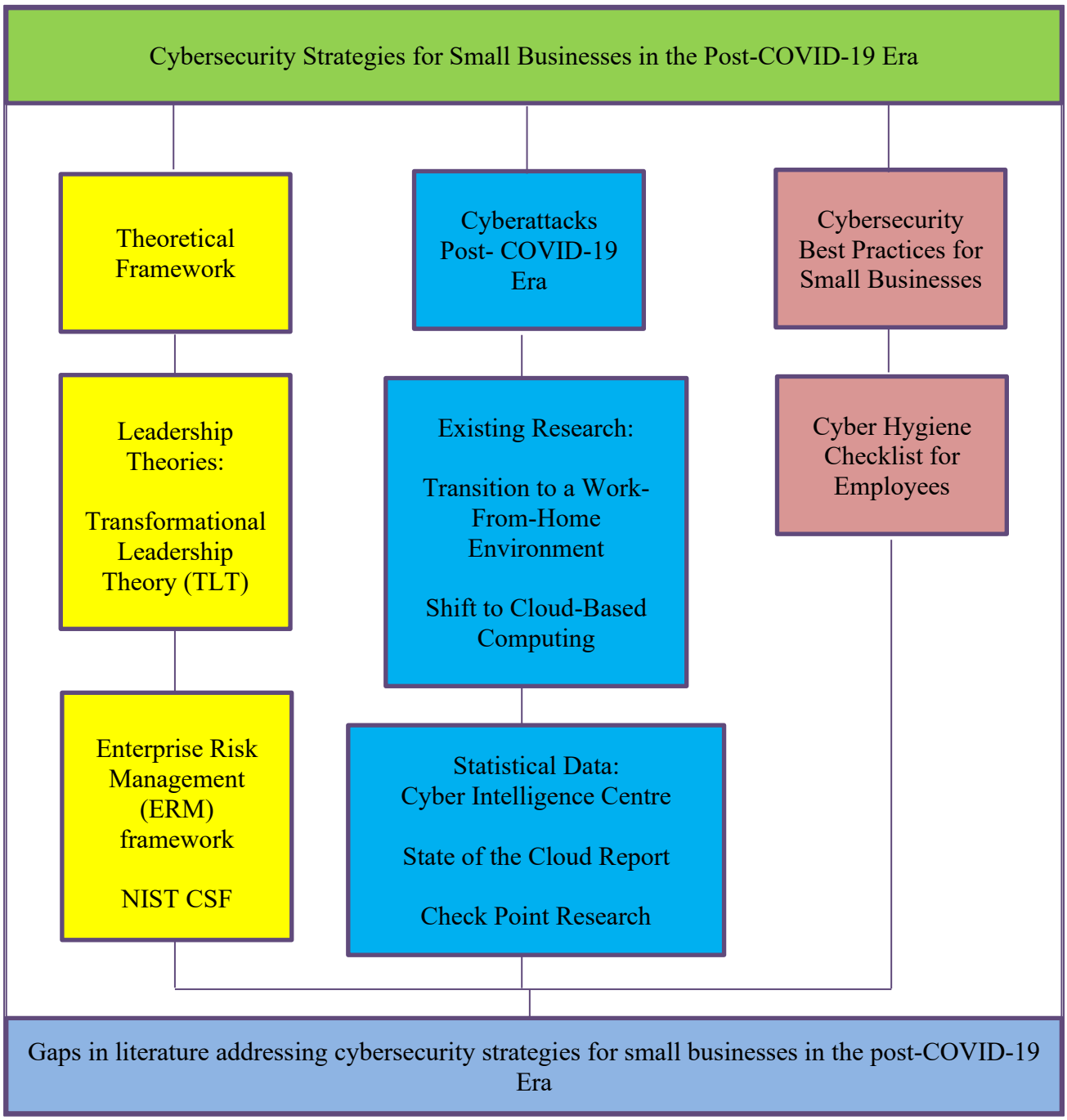
The conceptual framework served as a visual reminder of the study's focus as well as its foundational theories. The supporting literature for the two foundational theories, Enterprise Risk Management (ERM) framework and Transformational Leadership Theory (TLT), is represented by this map. By visually organizing these theories, researchers can better understand how they relate to each other and the overall study. The conceptual framework served not only as a visual representation of the study's focus but also as a structured guide for understanding how the key theoretical components interconnect and support the research objectives. Specifically, the framework illustrates the integration of ERM and TLT—two foundational pillars that inform both the problem being investigated and the

potential solutions. This tool helps researchers stay organized and ensures that all aspects of the study are thoroughly explored. By visually mapping out the connections between theories and literature, researchers can identify gaps in knowledge and areas for further exploration. Additionally, the conceptual framework can assist researchers in identifying gaps in existing literature and areas for further investigation. It also provides a clear roadmap for data collection and analysis, ensuring that each part of the study aligns with its theoretical underpinnings. Ultimately, the conceptual framework acts as both a navigational tool and a theoretical blueprint, grounding the research in well-established models while clarifying the relationships between key variables.

Figure 2 depicts the conceptual framework of major theories of cyberattacks, which lays the groundwork for Chapter 2. It provides a clear structure for organizing data and analyzing findings, ultimately contributing to a more coherent and comprehensive research study. The conceptual framework covers the potential impact of increased reliance on digital platforms and remote work arrangements on cybersecurity vulnerabilities. This comprehensive analysis sets the stage for a more profound understanding of the evolving landscape of cyber threats in the post-COVID-19 era. Small businesses should adhere to industry-wide cybersecurity best practices and implement a cyber hygiene checklist for employees. By implementing these measures, small businesses can better protect themselves from potential cyber threats and ensure the security of their digital assets in the ever-changing cybersecurity landscape.

Figure 2.

Conceptual Framework of Major Theories of Cyberattacks



Purpose of Study

The purpose of this qualitative study was to explore cybersecurity strategies that small business leaders implement to protect their businesses from cyberattacks in the post-COVID-19 environment. At this time “cybersecurity strategies” is defined as the implementation of comprehensive measures and protocols to protect computer systems, networks, and data from unauthorized access, breaches, and cyber threats. These strategies involved a combination of technological solutions, such as firewalls and encryption, as well as employee training and awareness programs to ensure that all individuals within an organization are equipped with the knowledge and skills to identify and respond to potential security risks. Additionally, cybersecurity strategies also encompass the regular monitoring and updating of security systems to stay ahead of evolving threats in the digital landscape. Businesses considered "small" consist of companies with fewer than 500 employees and often have limited resources for cybersecurity measures. The research population consists of small business leaders located in the greater Seattle metropolitan area.

Central Question

What cybersecurity strategies do small business leaders implement to protect and defend their businesses from cyberattacks?

Sub Problems

1. What cybersecurity strategies do small business leaders use for preventing, detecting, and responding to cyberattacks?
2. How can cybersecurity strategies adequately address the post-COVID-19 cyberattacks on small business cyberspace?

3. What cybersecurity strategies do small business leaders find most effective in mitigating risk from cyberattacks in their businesses?
4. What type of training programs does small business leaders offer for employees to educate them on security, data privacy, and compliance?
5. What best practices can business leaders implement to ensure their employees receive cybersecurity training?

Definition of Terms

The definition of key terminology ensures that the reader has a clear understanding of how terms are used throughout the study. The key terms to be used in this research are defined as follows.

Bring your own device (BYOD): the practice of businesses allowing staff to access business IT resources, including applications and data, via personal mobile devices like cellphones, laptops, and tablets (Ogie, 2016). In this study, BYOD refers to the growing trend of employees using their personal devices for work purposes.

Chief Information Security Officer (CISO): a senior executive who is responsible for establishing and maintaining organizational information security concerns that is consistent with the organization's global strategy (Dhillon, Syed, & de Sá-Soares, 2017). *CISO* is largely used in this study to refer to key experts who are knowledgeable about all aspects of information security (Whitman & Mattord, 2018).

Cloud Computing: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or interaction from service providers." (Xu, 2012, p. 2). In this study,

cloud computing refers to the practice of storing and accessing data and applications over the Internet instead of on a local server or personal device by small businesses.

COVID-19: a term used to refer to novel coronavirus disease 2019, is a mild to severe infectious disease caused by the SARS-CoV-2 virus, which was originally identified in China in 2019 and became a pandemic in 2020 (WHO, 2020). In this study, the term "pandemic" is used synonymously with the term "COVID-19." This study will define the pre-pandemic era before March 11, 2020; the pandemic period between March 11, 2020, and May 5, 2023; and the post-pandemic period, which will be considered after May 5, 2023.

Cyberattack: an intentional action taken to change, disrupt, deceive, degrade, or destroy computer systems or networks to gain access to information, resulting in data loss (Caplan, 2013). In this study, cyberattack refers to any malicious activity that targets computer systems or networks of small businesses to cause harm or extract valuable data.

Cybersecurity: a term often used interchangeably with the term *"information" security*, and involves a set of tools, policies, security concepts, security precautions, strategies, guidelines, risk management approaches, actions, training, best practices, guarantees, and technologies that can be used to safeguard the cyber environment, the organization, and user data (Solms & Niekerk, 2013).

Cybersecurity Strategies: the implementation of comprehensive measures and protocols to protect computer systems, networks, and data from unauthorized access, breaches, and cyber threats (Bryan, 2020). In this study, effective cybersecurity strategies encompass comprehensive measures to protect computer systems and regular monitoring and updating of security systems to stay ahead of evolving threats in the digital landscape.

Implement: applying safe cybersecurity best practices such as using strong passwords, updating software, and turning on multi-factor authentication are the basics of what is referred to as “cyber hygiene” (Li & Liu, 2021). In this study, an implement refers to developing and executing tailored cybersecurity plans and processes to protect and maintain business operations.

Protect and Defend: is a coordinated act of resistance that protects information, systems, and networks from cyberattacks by putting in place protective procedures such as firewalls, network detection and response (NDR), and endpoint detection and response (EDR) to identify, analyze, and report network-related incidents (IronNet, 2024). In this study, "protect and defend" refers to a coordinated act of resistance and implementation of policies and tools that help mitigate cybersecurity threats by small business leaders.

Risk: refers to the potential for loss, damage, or disruption to an organization’s assets, operations, or objectives resulting from the exploitation of vulnerabilities by threats (NIST, 2018). In cybersecurity, risk is typically understood as a function of the likelihood of a threat occurring and the potential impact of that event.

Threat: is any circumstance or event with the potential to exploit vulnerabilities and cause harm to an information system, organization, or its assets. Threats may be intentional (e.g., cyberattacks) or unintentional (e.g., human error or system failure) (NIST, 2018).

Small Business: a business for profit, independently owned, and primarily operated within the United States; a business with 500 or fewer employees and annual sales of up to $38.5 million contributes to the US economy through taxation and job creation (Buculescu, 2013). For this research, small businesses refer to firms having fewer than 500 employees located in the greater Seattle metropolitan area.

Small Business Leaders: individuals who have the vision and drive to start and grow a successful business, often taking on multiple roles within their company managing the implementation of strategy, policy, and technology, such as a CEO, CIO, CISO, IT director, IT manager, or general manager (Hickman & Akdere, 2018). In this study, small business leaders refer to business leaders located in the greater Seattle, WA, metropolitan area who are responsible for making strategic decisions, managing resources, and leading their teams to achieve goals.

The Northwest region of the United States: is commonly known as the Pacific Northwest (PNW) and primarily includes Washington, Oregon, and Idaho because of their shared economic and environmental characteristics.

Delimitations

Delimitations are the boundaries intentionally set by the researcher to define the scope of a study (Snelson, 2016). Unlike limitations, which are beyond the researcher's control, delimitations are purposeful decisions made by the researcher (Korrapati, 2016). In this study, delimitations included the sample, organizational size, and geographic scope.

First, the sample was limited to small business leaders operating in the post-COVID-19 era; individuals whose businesses were not active during the study period were excluded. Second, to ensure consistency and relevance of findings, the study focused only on organizations classified as small businesses by the Small Business Administration (SBA). Third, the geographic scope was restricted to the Pacific Northwest region of the United States, specifically the Seattle metropolitan area, selected based on accessibility and feasibility, consistent with recommendations by Creswell and Creswell (2022).

Assumptions

This study was based on four assumptions. The first assumption was that semi-structured interviews would provide sufficient data to answer the research questions, which was sufficient for triangulation and included sufficient detail and feedback to provide the necessary data for completing the study. The second assumption was that participants would understand the questions and provide honest and truthful answers, thereby increasing the study's validity and reliability. The third assumption was that for answering the research questions in this study, a qualitative approach was appropriate. The final assumption was that the rate of technological change would undoubtedly continue to accelerate, and small business leaders needed to develop capabilities to absorb continuous change and turn it into a source of competitive advantage, rather than simply adopting new technologies.

Significance of Study

Cybersecurity is a worldwide issue, and organizations across the globe require effective solutions tailored to their needs. Business leaders require robust strategies to mitigate the threat of cyberattacks (Meng et al., 2023). Data breaches lead to a greater loss of sensitive information, identity theft, and a decline in business profitability (Trumbach et al., 2023). Small businesses are increasingly becoming the targets of cyberattacks that, if not prevented, have the potential to shut down their operations, and this has become one of the most significant threats confronting companies today. Arpaci and Sevinc (2022) report that there has been a notable rise in cyberattacks in recent years, with a swift increase in the number of attacks globally and a corresponding rise in business costs. It is estimated that small business leaders require over $3.8 million to recover from a security breach (Ho et al., 2023). Currently, the United States (U.S.) government requires many small businesses under

contract to demonstrate their implementation of nationally mandated cybersecurity guidelines. In today's digitally connected world, all businesses should formulate a cybersecurity policy.

The study explored cybersecurity strategies for small businesses that are necessary to improve the protection of systems from data breaches. The results of this study should help small business owners better understand their cybersecurity vulnerabilities and devise robust cybersecurity policies and procedures to protect their systems from future data breaches. The analysis should provide important information about cybersecurity practices that small businesses can implement to prevent potential data breaches and attacks. The study continued to fill gaps in the understanding and practice of small business security. Previously, researchers focused on security in large corporations, ignoring small businesses as an important element in their literature.

This research has the potential to be a social change tool. By educating small business leaders this research can serve to accelerate the adoption of cybersecurity practices that can protect their systems from data breaches. The findings of this research could be useful for small business leaders who want to prevent and mitigate the cost of cyberattacks. The findings provided small businesses with operational strategies to protect themselves from a cyberattack, potentially lowering operational costs and increasing consumer confidence.

Chapter Two

Literature Review

Introduction

Cyberattacks have become a major global challenge and concern for small businesses. With the introduction of the Internet and new technologies, cybercriminals can now infiltrate individuals and businesses through their computer systems. Cybercriminals have increasingly targeted small businesses even before the COVID-19 pandemic, owing to a lack of resources to implement comprehensive cybersecurity solutions (Alawida et al., 2022). This report highlights how small businesses have been prime targets for cybercriminals due to their limited resources for cybersecurity, a trend that predates the COVID-19 pandemic. The shift to remote work, increased reliance on digital platforms, and disruptions to traditional business operations have created new vulnerabilities in both personal and organizational cybersecurity. The authors point out the need for robust cybersecurity measures and continuous education to address the challenges exacerbated by the COVID-19 pandemic.

A critical review of the literature informed the development of this qualitative study by examining prior research directly related to the research question being addressed in this study, allowing the researcher to identify cybersecurity strategies used by small business leaders to protect their systems from data breaches. This review identified key themes, methodological approaches, and gaps in existing literature, providing a foundation for the study's purpose and design. This section also endeavors to encompass a range of research that aligns with the theoretical framework guiding this question. The literature review seeks to identify potential areas for future research on cybersecurity threats. As a result, the risks of cloud computing and BYOD will be thoroughly discussed.

The Importance of Cybersecurity for Small Businesses

Cybersecurity is all about protecting an organization's data from attacks by both internal and external malicious actors. It can refer to a set of technologies, processes, structures, and practices used to safeguard networks, computers, programs, and data from unauthorized access or damage (Lundgren & Möller, 2019). A single security breach can expose millions of people's personal information and jeopardize confidentiality, data integrity, and availability (collectively known as the CIA triad) of business information, which are fundamental information security principles (Gera et al., 2025). These breaches have a significant financial impact on businesses and result in a loss of customer trust (IBM Security, 2023). Therefore, cybersecurity is vitally important to safeguard individuals and organizations from cybercriminals. To stay ahead of evolving threats and vulnerabilities, organizations should constantly update and adapt their cybersecurity measures (Verizon, 2021). Organizations that prioritize cybersecurity can reduce the risk of data breaches, financial losses, and reputational damage.

Small businesses are a vital component of the U.S. economy, accounting for 43.5% of GDP and employing 46% of the private-sector workforce (SBA, 2023). According to the SBA Office of Advocacy, there are 33.3 million small businesses in the United States, making up 99.9% of all businesses. Among these, approximately 27 million operate as sole proprietorships. Between 1995 and 2021, small businesses generated 17.3 million new jobs, representing 63% of total job growth. Additionally, small businesses account for 32.6% of total U.S. exports, valued at $413.3 billion, and make up 97.3% of all exporting firms (U.S. Census Bureau, 2022). According to McIntyre (2019), the majority of U.S. businesses—

approximately 89.6%—have fewer than 20 employees, reinforcing the dominance of small enterprises in the national economy.

Cyberattacks impose significant financial burdens on the U.S. economy, costing hundreds of billions of dollars annually. In 2021, cybercrime losses in the U.S. reached $6.9 billion, with over 847,000 reported incidents (FBI Internet Crime Report, 2021). Cybersecurity Ventures (2023) projects that global cybercrime damages will increase from $3 trillion in 2015 to $10.5 trillion annually by 2025. The President's Budget for 2023 allocated $15.6 billion for cybersecurity initiatives, demonstrating the growing financial commitment to national cybersecurity (White House, 2023). Cyberattacks on businesses and individuals continue to rise, with the global cost of cybercrime expected to exceed $20 trillion by 2026, a 150% increase from 2022 levels (Statista, 2023).

IBM and the Ponemon Institute reported that the average cost of a data breach in 2022 reached $4.35 million, marking a 12.7% increase compared to the 2020 report (Ponemon Institute, 2022). Experts predict that typical data breach expenses could surpass $5 million by 2023. The study takes into account various costs, including legal, regulatory, technical, brand equity loss, customer turnover, and employee productivity drain. This report is based on an analysis of 550 breaches across 17 countries and industries, with data gathered from over 3,600 interviews. The research also found that the cost per record compromised during a breach has risen to $175, further highlighting the increasing financial burden on businesses. These findings emphasize the critical need for organizations to invest in robust cybersecurity measures and incident response plans to mitigate the financial damage caused by such breaches (Ponemon Institute, 2022).

In the contemporary interconnected and competitive landscape, safeguarding clients' personal information remains an ongoing challenge for businesses. Cybercriminals target small businesses daily because they have sensitive information and must protect themselves and their customers (SBA, 2021). Small businesses face challenges in their ability and desire to protect themselves against cyberattacks, making them particularly vulnerable. Over 700,000 attacks on small businesses occurred in 2020 alone, with damage totaling $2.8 billion, and the figures continue to climb yearly (Madrid, 2021). Large corporations use enormous resources to protect themselves from cyberattacks by outsourcing these services or establishing their own cybersecurity department (Muravskyi et al., 2021). Hackers are aware that small businesses cannot afford to invest as much.

El-Hajj and Mirza (2024) focused on addressing the unique cybersecurity challenges faced by small and medium enterprises (SMEs). Recognizing that SMEs often lack the resources and expertise to implement comprehensive cybersecurity measures, the authors propose a specialized risk assessment framework and tool tailored to the needs of these organizations. The proposed framework serves as a practical resource to help SMEs navigate the complexities of cybersecurity in a way that is both accessible and actionable. While the framework and tool are well-defined, there is limited empirical testing or real-world case studies to demonstrate the effectiveness and practical application of the proposed model.

Cybercrime is constantly changing as the Internet develops and changes. Things that were not possible ten years ago are now possible, altering the landscape. Data breaches can significantly impact a company's reputation and consumer confidence. Approximately 59% of small and medium-sized businesses in the United States lack a contingency plan that delineates the protocols for addressing and disclosing losses resulting from data breaches

(National Cybersecurity Alliance, 2021). It is crucial for organizations to prioritize cybersecurity measures and develop comprehensive contingency plans to mitigate potential damage and protect their reputation in the digital age.

Wong et al. (2022) further examined the role of cybersecurity awareness and policy comprehension in enhancing supply chain resilience among small and medium-sized enterprises (SMEs). Drawing on Protection Motivation Theory, the researchers surveyed 200 SMEs to assess how their understanding of cybersecurity practices and policies influenced organizational readiness and hygiene. Their findings indicate that SMEs with higher levels of awareness and structured cybersecurity policies were better equipped to respond to threats, thereby minimizing disruption and potential data loss. The study emphasizes the necessity of embedding cybersecurity awareness into organizational culture and prioritizing preventive strategies—especially employee training—as critical components in mitigating cyber risks in an increasingly digitized post-pandemic environment. This argument is further supported by Wilson et al. (2023), whose survey on cybersecurity attitudes among UK SMEs revealed a prevailing belief that they are unlikely to become targets of cyberattacks. A reactive approach to cyber defense results from this false sense of security. Additionally, Chidukwani et al. (2022) found that SME commitment to cybersecurity can diminish over time, particularly when there are no immediate or visible benefits from their efforts. This gradual erosion in vigilance often results in underinvestment in crucial areas, such as employee training, system upgrades, and incident response planning, thereby increasing long-term exposure to cyber risks.

The Role of the Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA), established in 2018 under the Department of Homeland Security (DHS), plays a pivotal role in the protection of the nation's critical infrastructure against cyber threats. As the lead federal agency for cybersecurity, CISA provides centralized coordination for threat detection, prevention, and response across both public and private sectors. For small businesses that often operate with limited resources and lack in-house cybersecurity expertise, CISA's publicly available toolkits—such as the "Cyber Essentials" guide—serve as a foundational roadmap for implementing basic cyber hygiene practices and building a security-conscious culture (CISA, 2023).

In the context of this paper, incorporating CISA is essential for understanding the federal landscape of cybersecurity governance. CISA's frameworks and guidance documents influence national standards and organizational practices, making its role foundational to the broader conversation about cyber risk management, regulatory compliance, and resilience-building within critical infrastructure sectors. CISA's initiatives include the Continuous Diagnostics and Mitigation (CDM) program, which equips federal agencies with tools to identify, prioritize, and mitigate cybersecurity risks. Furthermore, the agency regularly issues alerts, conducts assessments, and facilitates rapid incident response in collaboration with both governmental and private entities.

In the post-COVID-19 era, small businesses have become increasingly vulnerable to cyber threats due to expanded remote work, cloud adoption, and limited IT resources. Recognizing this, CISA has prioritized outreach and support to help SMEs strengthen their cybersecurity posture. Through its *Cyber Essentials* initiative, CISA offers a set of basic

guidelines tailored for small businesses, focusing on foundational cyber hygiene practices such as securing email systems, maintaining backups, and training employees to recognize phishing attacks. CISA has also released sector-specific resources and hosted virtual workshops during and after the pandemic to help small businesses adapt to new threat landscapes (CISA, 2021). These efforts reflect a broader strategic shift by the agency to ensure that national cybersecurity resilience includes not only large critical infrastructure providers but also the smaller organizations that form the backbone of the U.S. economy.

COVID-19 Pandemic Impacts on Cybersecurity

The pattern of cybercrime committed pre-COVID and during COVID-19 should be considered if any conclusions can be drawn from these data. Analyzing how cybercrime has changed since the pandemic's start is crucial to understanding COVID-19's effects (Grampp et al., 2020). The COVID-19 pandemic considerably impacted cybercrime and understanding the data analysis requires examining how cybercrime has evolved. As a result of the rapid acceptance of digital technologies, many elements of life have gone online, ranging from commerce and social connections to business, industry, and, tragically, criminality (Alouffi et al., 2021). This shift has created new opportunities for cybercriminals to exploit vulnerabilities and target individuals, businesses, and even governments. With the increase in online activity, there has been a corresponding rise in cyberattacks, fraud, and data breaches. As we continue to navigate the digital landscape, it is essential to stay vigilant and implement robust cybersecurity measures to protect against evolving cyber threats.

Figure 3 illustrates the negative effects of the pandemic on cybersecurity, and we detail each impact below. As the pandemic accelerated the global shift toward remote work and digital operations, businesses and individuals became more exposed to cyber threats. This period saw

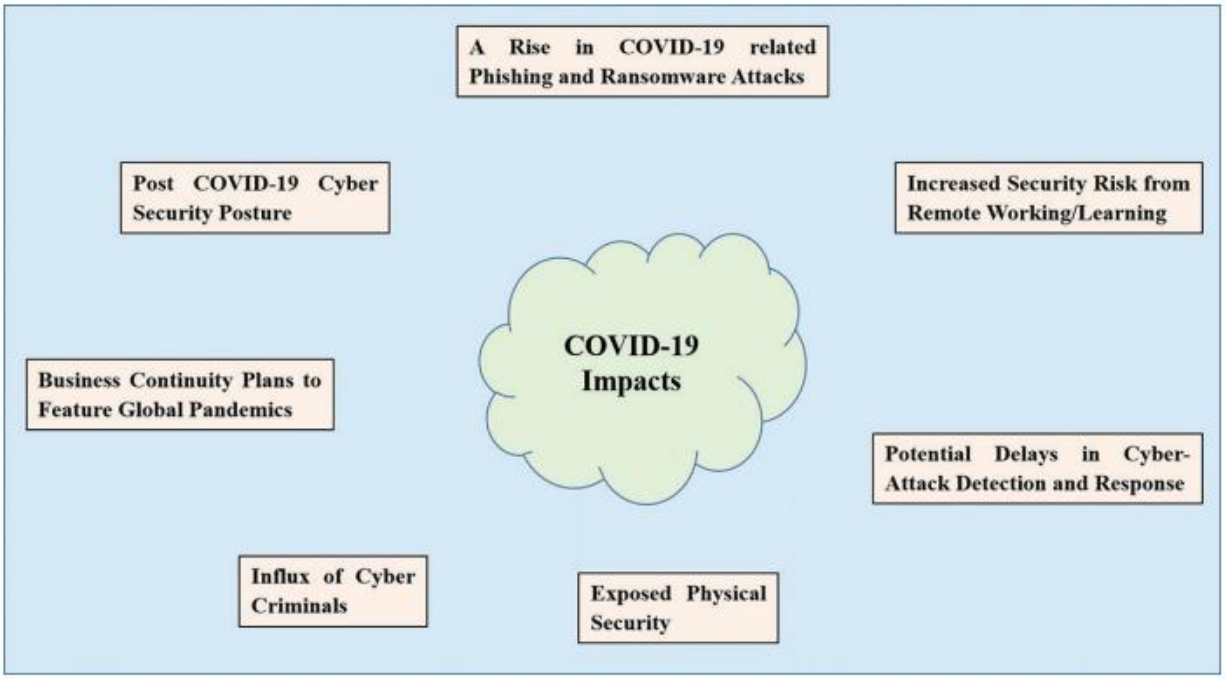
a marked increase in data breaches, phishing attacks, ransomware incidents, and other forms of cybercrime. Many organizations, particularly small businesses, struggled to adapt to these rapid changes, often lacking the resources or infrastructure necessary to secure their digital environments effectively. The surge in cyberattacks during the pandemic has driven home the urgent need for stronger cybersecurity protocols, greater employee awareness, and investment in secure technologies. These developments reveal not only the vulnerabilities exposed by the crisis but also the opportunity to learn and strengthen cybersecurity resilience. By understanding the specific challenges that arose during the pandemic, both organizations and individuals can take proactive steps to better defend against similar threats in the future, ensuring safer participation in an increasingly interconnected digital world.

Impact-1: A Rise in COVID-19-Related Phishing and Ransomware Attacks

The Cyber Intelligence Centre (2020) conducted a study examining the rise in phishing, malware, and ransomware attacks during the COVID-19 pandemic. The research focused on how cybercriminals exploited the global crisis to deceive individuals and organizations. Data collection occurred in the early months of the pandemic, from March to June 2020, when remote work became widespread, increasing cybersecurity vulnerabilities. The study gathered data through a combination of cybersecurity incident reports, surveys, and real-time threat intelligence monitoring. It analyzed thousands of phishing emails and malware-infected links that targeted employees and customers of various organizations. The findings indicated a significant increase in COVID-19-themed cyberattacks, where hackers spoofed trusted brands and government agencies to distribute malicious content.

Figure 3

COVID-19 cybersecurity impacts



One key component of the study was a survey conducted among 500 IT professionals and security experts across multiple industries. The survey results revealed that 68% of organizations experienced an increase in phishing attacks; 52% of respondents reported incidents of malware or ransomware disguised as COVID-19-related updates or applications, and 41% of IT professionals admitted that their organization was not fully prepared to handle the sudden surge in cyber threats. The study concluded that organizations and end-users must remain vigilant against COVID-19-related ransomware and phishing scams. It is recommended that businesses implement strict cybersecurity awareness programs, improve email filtering, and enforce MFA to mitigate risks. Additionally, employees and consumers were advised to be cautious when accessing links, emails, or downloading documents that claim to provide pandemic-related information. By outlining these findings, the study points

out the urgent need for enhanced cybersecurity measures and greater awareness to protect against evolving cyber threats.

COVID-19 emerged in an already complex cybersecurity landscape at the beginning of 2020, acting as a catalyst for digital transformation and accelerating human adaptability (IBM Security, 2022; Verizon, 2023). As businesses and individuals rapidly shifted to remote work and digital communication, phishing and ransomware attacks related to COVID-19 surged exponentially, exploiting the heightened demand for timely information and news dissemination (CISA, 2021). Threat actors leveraged pandemic-related themes to deceive users through email scams, fraudulent websites, and malicious applications, leading to an increase in cyberattacks targeting both organizations and individuals.

The digital landscape experienced an extraordinary increase in cyberattacks globally during the third quarter of 2024 (see Fig. 4). This period saw a notable increase in the volume and intensity of cyber threats that organizations encounter, highlighting the evolving tactics of cybercriminals and the pressing necessity for strengthened cyber defenses. In the third quarter of 2024, the average weekly cyberattacks per organization reached an unprecedented level of 1,876, representing a remarkable 75% rise compared to the same timeframe in 2023 and a 15% increase from the preceding quarter (Check Point, 2024). This increase highlights the growing prevalence and complexity of virtual threats.

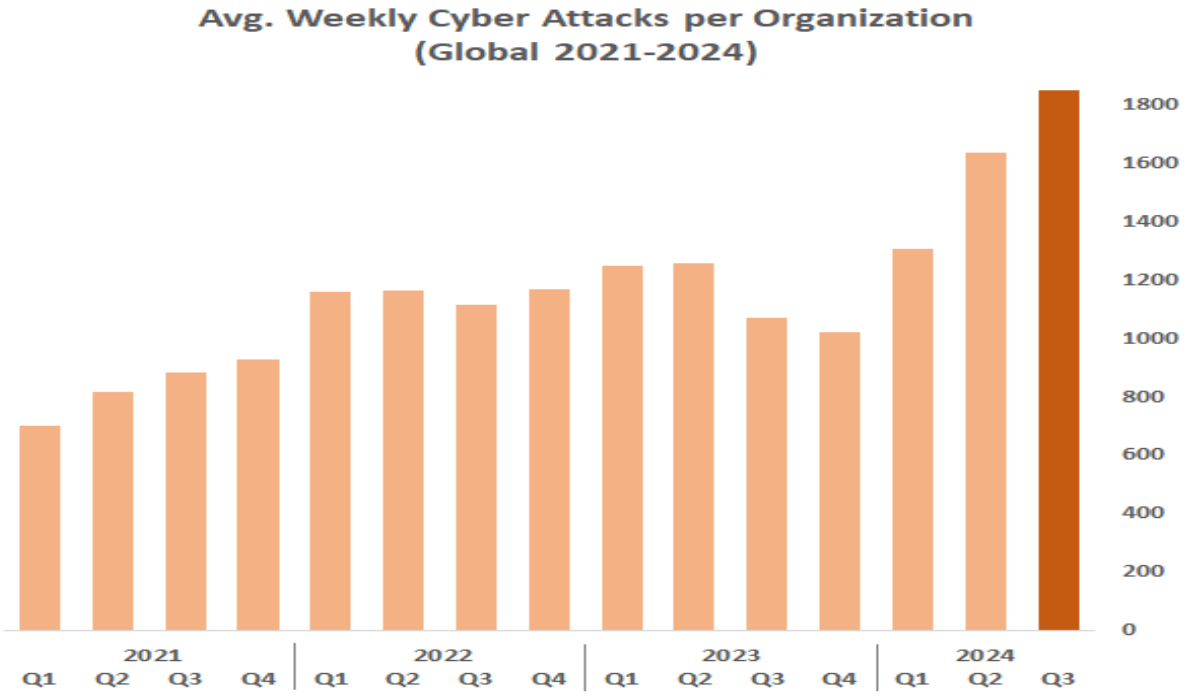
Impact-2: Increased Security Risk from Remote Working/Learning

Businesses and schools now rely on Virtual Private Network (VPN) servers because many employees work from home and students learn online. Their security and access will be a big focus in the future (TCS Worldwide, 2023). Some people may use their personal computers for work-related tasks, which can pose security risks to organizations.

Organizations should ensure the safety and effectiveness of VPN services, given the likely scrutiny they will face.

Figure 4.

Global Cyberattacks 2021-2024



Note. Adapted from Check Point Q3 2024 Report

According to Alawida et al. (2022), email-based phishing threats were the most prevalent cause of data breaches because of the COVID-19 pandemic-induced increase in people working from home. In addition, a study conducted by Deloitte involving 1,500 Swiss residents of working age revealed that 25% had encountered an increase in phishing/spam/fraudulent emails since the outbreak of COVID-19 (Deloitte, 2022). Notable is the fact that nearly half of the respondents reported working from home due to the pandemic (Grampp et al., 2020).

Impact-3: Potential Delays in Cyber-Attack Detection and Response

The operation of various security teams is likely to be affected because of the COVID-19 epidemic, making it difficult to identify malicious activity and even harder to respond to (Deloitte, 2022). If security teams are not operational, updating device fixes can present a challenge. Organizations should examine their security defenses and consider using co-sourcing with external experts, especially in areas where significant human risks have been identified.

By leveraging external expertise, organizations can benefit from the specialized knowledge and resources needed to address emerging threats during this challenging time. Collaborating with outside security teams can provide a fresh perspective and help fill in any gaps in internal capabilities. In doing so, organizations can enhance their overall security posture and better protect themselves against cyber threats amidst the ongoing disruptions caused by the pandemic.

Impact-4: Influx of Cybercriminals

To address the effects of COVID-19, organizations worldwide are decreasing their personnel. Most professionals have lost their jobs due to global travel restrictions. This approach would undoubtedly foster the proliferation of cyber thieves, as idle people with Internet connections who have lost their employment due to the consequences of COVID-19 may see this pandemic as an opportunity to make a living (Alouffi et al., 2021).

Companies that are considering layoffs should implement proper exit strategies. These strategies should include providing support and resources for employees who are being let go, such as access to mental health services and assistance in finding new job opportunities. By taking care of their employees even during the difficult process of downsizing, companies can

help prevent them from turning to unethical means to support themselves. It is crucial for organizations to prioritize the well-being of their employees, even in times of crisis, to maintain a positive and ethical work culture.

Impact-5: Post-COVID-19 Cyber Security Posture

The COVID-19 pandemic has significantly strained the global economy, with some analysts predicting a recession as one of the pandemic's aftereffects (Deloitte, 2020). Organizations are downsizing by eliminating business divisions to reduce economic losses in this situation. This category also encompasses cybersecurity operations deemed to be non-critical. It is recommended that organizations upgrade their remote working policies/practices when prioritizing cybersecurity during the re-strategize phase following COVID-19 (Borkovich & Skeviri, 2022). The fight against COVID-19 is not only for business, employees, or clients but a collective effort from everyone.

Reputable research organizations employ diverse methodologies to conduct comprehensive cybersecurity reports. Check Point Research (2025) has released its latest findings on cyberattack trends, revealing that cyber threats continue to escalate globally. In response to ongoing geopolitical conflicts, including the Russia-Ukraine war and tensions in the Asia-Pacific region, cyberattacks have reached unprecedented levels, with threat actors leveraging AI-driven malware, zero-day exploits, and cloud vulnerabilities to compromise organizations.

According to the Check Point 2025 Cyber Security Report, cyberattacks increased by 42% in 2024 compared to the previous year, with an average of 1,320 weekly attacks per organization worldwide. Ransomware attacks remain one of the most financially damaging threats, with a 60% rise in double extortion tactics. The education and research sectors

continue to be among the most targeted industries, while attacks on the healthcare sector surged by 81% annually, highlighting the persistent risks to critical infrastructure and patient data security (Check Point Research, 2025). Additionally, the rise of deepfake technology, social engineering attacks, and supply chain vulnerabilities has further complicated cybersecurity defense strategies. Organizations are increasingly shifting towards zero-trust architectures, AI-enhanced security solutions, and robust cloud security frameworks to mitigate evolving threats (Check Point Research, 2025).

Hashmi et al. (2024) explored the evolving intersection of AI and information security by providing an in-depth survey of how AI technologies are being integrated into cybersecurity strategies to enhance threat detection, risk management, and response times. AI systems can analyze large volumes of data more efficiently than traditional methods, allowing for quicker identification of emerging threats. Furthermore, it is important to ensure that AI-driven security solutions are transparent, accountable, and robust against manipulation. In conclusion, the article emphasizes the promise of AI to strengthen cybersecurity while acknowledging the need for ongoing research and careful implementation to avoid potential risks.

How COVID-19 has Shifted the Cybersecurity Threat Landscape

The COVID-19 pandemic has necessitated a transition to remote work, significantly increasing the number of employees working from home. Before the pandemic, only 6% of Chicago residents reported working full-time from home. In the spring of 2020, however, it was reported that 90% of full-time employees were working from home at least four days per week, and 62% expressed a desire to continue doing so in the future (Conway et al., 2020). Cybersecurity has emerged as a top priority due to the widespread transition to working from

home. The COVID-19 pandemic's influence on the shift to cloud computing has further altered the cybersecurity threat landscape. According to Alouffi et al. (2021), cloud computing aims to provide hosted services over the Internet that are not controlled by the provider.

Transition to a Work-From-Home Environment

We must investigate the effects of COVID-19 and the transformation of the cyber threat landscape. The world immediately shifted from a predominantly in-person office environment to a predominantly at-home workplace. Due to imminent health concerns, these changes were drastically accelerated, and when change is rushed, security holes are exposed (Pizzo, 2023). While some employees in various industries were already able to work from home, most cases relied on specific procedures and policies to ensure their security. In the event of the mass transition to a work-from-home environment, these policies and procedures, if they existed, did not consider the potential technological incapacity of the employees or the large number of employees who were subject to them (Borkovich & Skeviri, 2020). In a state of emergency, such as the COVID-19 pandemic, acquiring devices that could be securely transported home from the office was virtually impossible unless they were owned (Eiza et al., 2021).

Bring Your Own Device (BYOD)—also referred to as Bring Your Own Technology (BYOT) or Bring Your Own Phone (BYOP)—is a workplace policy that permits employees to use personal devices for professional tasks (Palanisamy, 2020). A common example of BYOD is when an organization allows employees to access corporate email or applications on their personal smartphones, tablets, or laptops. While BYOD enhances workplace flexibility

and productivity, it also introduces significant cybersecurity risks, including data breaches, malware infections, and unauthorized access to corporate networks.

Research by Gaff (2015) initially examined BYOD from the perspectives of productivity gains and organizational risk. More recent studies emphasize that BYOD policies can increase an organization's exposure to cyber threats, particularly in hybrid or remote work environments where endpoint security is more difficult to enforce (Ogungbemi, 2024). To mitigate these risks, organizations must implement a comprehensive BYOD security policy, incorporating MFA, mobile device management (MDM) solutions, data encryption, and employee cybersecurity training (Rah, 2023).

BYOD provides numerous benefits to enterprises and employees, including greater employee productivity, contentment, effectiveness, and cost savings to companies and IT departments for hardware, software, licensing, and maintenance (Del Vecchio, 2021). Remote working poses obstacles and exposes various social engineering cyberattacks and cybersecurity issues via emails, file sharing, and network access via user devices (Pizzo, 2023). Home networks continue to be less secure than organizational internal networks, perhaps posing greater risks to employees already vulnerable to cyberattacks.

The COVID-19 pandemic touched all organizations worldwide, forcing them to rethink and redesign new approaches to move to the new environment of remote work (Rah, 2023). Because firms rely on information technology for business continuity and communication, the transition to working from home has increased its importance (Sarma, 2022). The COVID-19 pandemic accelerated BYOD, which was already moving quickly. Working from home gave BYOD another vulnerability (Kashyap, 2021). Cybercriminals exploited the global shift to remote work during the COVID-19 pandemic, launching both

indiscriminate and targeted attacks. This transition exposed the lack of preparedness among many vendors, particularly regarding the effectiveness of their security products (Lallie et al., 2021). The sudden, large-scale move to remote work also led to a surge in the use of digital technologies (Rahul De' et al., 2020).

Studies by Hijji and Alam (2021) and Lallie et al. (2021) demonstrate that the frequency and sophistication of cyberattacks increased significantly during the pandemic, with heightened public anxiety further exacerbating vulnerabilities. Wong et al. (2022), using Protection Motivation Theory, explored the impact of general cybersecurity awareness and cybersecurity policy knowledge on enhancing reactive capabilities within supply chain resilience. By surveying 200 small and medium-sized enterprises (SMEs), the study found that strong cybersecurity awareness and policy adherence significantly improve an organization's overall cyber hygiene. These findings demonstrate the vital role of proactive cybersecurity measures and employee education in reducing the risk and impact of cyberattacks.

Shift to Cloud-Based Computing

Understanding malicious websites is crucial for a company's digital security strategy, especially with the increasing reliance on cloud computing, which introduces new cybersecurity risks. Malicious websites are used for phishing, malware distribution, and data breaches, often leveraging cloud services to evade detection and target businesses (Jimmy, 2024). As cloud computing continues to expand, companies must enhance their security frameworks to protect against web-based cyber threats. The pandemic and the rising demand for flexibility have driven many organizations towards cloud-based infrastructure solutions rather than on-premises infrastructure. Modern cyber threats, such as phishing, malware

distribution, and data exfiltration, are increasingly deployed through malicious websites, making it imperative for organizations to detect, analyze, and mitigate these threats (Alouffi et al., 2021). The authors conducted a thorough systematic review of the existing literature on cloud computing security. They identified and categorized the primary threats to cloud computing, such as data breaches, unauthorized access, data loss, and denial-of-service attacks. The authors did not focus on specific geographical regions or industries, such as small businesses in particular areas, like the Western United States.

Businesses use cloud computing directly and indirectly, and if a security compromise occurs, a company may experience escalating and long-lasting consequences. This contemporary trend in IT infrastructure has been prevalent for several years, with Amazon's AWS and Microsoft's Azure serving as industry leaders (Pizzo, 2023). The COVID-19 pandemic and the increasing demand for flexibility have accelerated the adoption of cloud-based infrastructure solutions over traditional on-premises systems. This shift has both positive and negative security implications, but overall, cloud adoption has provided scalability, remote accessibility, and cost efficiency for businesses. The mass migration to cloud computing is expected to continue growing, with a projected compound annual growth rate (CAGR) of 22.59% between 2019 and 2022 (Alashhab et al., 2021). However, this rapid expansion also introduces new cybersecurity risks, including data breaches, misconfigurations, and increased attack surfaces.

Cloud computing has rapidly evolved, attracting a diverse range of users from various industries, disciplines, and global regions. During the COVID-19 pandemic, cloud technology played a crucial role in supporting government and business operations, ensuring continuity in education, healthcare, industry, communication, and remote surveillance (Alouffi et al.,

2021). According to a recent survey by Flexera (2023), 27% of business leaders reported a significant increase in cloud spending due to the pandemic's effects, demonstrating the growing reliance on cloud-based infrastructure.

Despite its advantages, cloud computing also introduces cybersecurity vulnerabilities (Jimmy, 2024). Organizations that adopt cloud solutions often share data centers located worldwide, leading to increased risks such as data leaks, unauthorized access, and security misconfigurations (Shobana et al., 2022). Misconfigurations and human errors are among the leading causes of data breaches in cloud environments, making cybersecurity measures a top priority for businesses shifting to cloud-based models (Tabrizchi & Rafsanjani, 2020).

Best Cybersecurity Practices for Small Businesses

Before getting into cybersecurity best practices for small businesses, it is critical to understand the common methods used by cybercriminals to infiltrate their targets. Understanding these tactics will help small businesses better protect themselves from potential threats and vulnerabilities in their cybersecurity measures. By knowing how cybercriminals operate, businesses can proactively implement effective security measures to safeguard their data and systems. Cybersecurity professionals continue to acknowledge two primary classifications of cybercrime. Computer-as-a-target crimes involve attacks on computer systems or networks, whereas computer-as-a-tool crimes involve the use of computers to carry out traditional illegal acts. Computer-as-a-target crimes involve attacks on computer systems or networks, while computer-as-a-tool crimes involve using computers to facilitate traditional criminal activities. Accordingly, cybercriminals may infect computers with viruses first, then utilize those infected computers to spread malware over a network or to other workstations (Khweiled et al., 2021). Table 2 shows the most common techniques

used by cybercriminals, which include denial of service, man-in-the-middle attacks, malware, and phishing. Additionally, ransomware attacks have become increasingly common in recent years.

Table 2

Methods Commonly Used by Cybercriminals

Method	**Description**	**Reference**
Denial of Service	A hacker consumes all server resources, so access to the service is not possible for system users.	Alghamdie (2021)
Man-in-the-Middle	Where a hacker puts himself between the victim device and the router to eavesdrop on or change data packets.	Huang et al. (2020)
Malware	Malware is a way in which victims come in contact with worms or viruses and their devices become infected.	Edgar and Manz (2017)
Phishing	It is a method in which a hacker sends a seemingly legitimate email asking users to disclose confidential information.	Saxena and Gayathri (2021)

Source: Adapted from Li & Liu (2021), see Appendix F for request for permission from the authors

As cyberattacks become more sophisticated and pervasive, businesses and individuals must adopt basic cyber-hygiene practices to mitigate the risk of common cyber threats (Nifakos et al., 2021). Preventing cyberattacks, particularly repeated breaches, is essential for businesses, as a single incident can result in significant financial and reputational damage. While businesses implement security measures to protect sensitive data, cybercriminals continually exploit vulnerabilities, leading to the exposure of millions of customer records and financial losses reaching billions of dollars (Perwej et al., 2021). The COVID-19 pandemic exposed the cybersecurity weaknesses of many organizations, leading them to implement proactive security strategies to prepare for future threats. Lessons from the pandemic should

drive businesses to strengthen their cybersecurity frameworks by investing in employee training, secure network infrastructure, and robust threat detection systems.

Small businesses should adopt proactive cybersecurity measures to minimize the impact of cyberattacks, including investing in a cybersecurity response team and developing a comprehensive incident recovery plan (Perwej et al., 2021). Research indicates that small businesses that enhance their cybersecurity posture are those that integrate cybersecurity preparedness into their daily operations. Experts recommend that small businesses implement key security strategies, such as conducting regular security risk assessments to identify vulnerabilities (Alghamdi, 2022), implementing employee training programs to mitigate human error and phishing threats, and keeping software and systems updated to protect against known exploits and vulnerabilities.

Ncubukezi (2023) explores the vulnerabilities of small businesses to cyberattacks by examining both planned and unplanned threats. The study employs a qualitative research methodology, including interviews and case studies of small business owners and cybersecurity professionals, to gather insights into the nature of cyber risks faced by these organizations. Through this approach, the research highlights that small businesses encounter heightened risks due to limited resources, insufficient cybersecurity expertise, and inadequate preventative measures. The study differentiates between planned cyberattacks—such as those executed by malicious hackers with specific objectives—and unplanned attacks, which arise from accidental breaches or human error. Ncubukezi emphasizes that small businesses are particularly vulnerable to both forms of cyber threats, often leading to significant financial losses and damage to reputation.

By adopting these cybersecurity best practices, small businesses can strengthen their defenses, minimize financial and reputational losses, and protect sensitive customer data (Chidukwani et al., 2022). Given the growing frequency and sophistication of cyber threats, prioritizing cybersecurity is essential for safeguarding business continuity and maintaining customer trust. By adopting these cybersecurity best practices, small businesses can strengthen their defenses, minimize financial and reputational losses, and protect sensitive customer data (Nifakos et al., 2021). Given the growing frequency and sophistication of cyber threats, prioritizing cybersecurity is essential for safeguarding business continuity and maintaining customer trust.

Implementing a strong password policy is the first and potentially most contentious step (Eiza et al., 2021). A strong password policy restricts common passwords and requires minimum password complexity, reducing the risk of brute-force attacks. Because a well-structured password cannot be easily guessed, malicious actors find it significantly harder to exploit this vulnerability. Continuing the topic of best practices for general account security, activating MFA is another crucial step toward organizational security. The fundamental principle behind MFA is that it requires users to authenticate their identity through multiple factors rather than just a single password. Such authentication can be accomplished through SMS, email, authenticator apps, or a physical security token as a secondary verification method (Suleski et al., 2023). MFA strengthens an organization's cybersecurity posture by adding multiple layers of defense, reducing the likelihood of unauthorized access, and mitigating threats associated with credential theft.

Businesses should implement employee education and awareness programs as a primary defense against cyberattacks on small businesses (Nguyen et al., 2023). Human

errors, such as mistyping an email address or failing to recognize phishing attempts, can lead to significant security breaches. To mitigate these risks, employees must receive extensive training in cybersecurity best practices and proper cyber hygiene. Studies show that organizations that conduct regular cybersecurity training sessions experience fewer successful cyberattacks compared to those that do not (Shillair et al., 2022). Training employees on phishing attack recognition, secure password practices, and incident escalation protocols can significantly strengthen an organization's security posture (Vadlamudi & De, 2021). Given the rapid escalation of cybercrime, relying solely on technological solutions is insufficient; a comprehensive security strategy must incorporate ongoing education and human-centric security measures.

Graham (2021) promotes the use of antivirus software, emphasizing that such programs must be configured to perform daily scans to ensure devices are protected against new threats. Regular scanning and updates place users in a stronger position to identify and mitigate cyber risks as they arise. Recent studies highlight that advanced anti-virus solutions, integrated with AI and machine learning, improve threat detection and response capabilities in real time (Vasani et al., 2023). Additionally, a combination of end-to-end encryption and VPNs requiring MFA is an effective method to secure company data handled by remote workers. This layered security approach offers greater protection than using a standard VPN alone. Furthermore, software and system updates, often overlooked, are essential cybersecurity measures.

Research indicates that cybercriminals frequently exploit unpatched vulnerabilities, making timely updates a critical defense mechanism (Dissanayake et al., 2021). The COVID-19 pandemic has intensified cybersecurity challenges by increasing the adoption of remote

work and bring-your-own-device (BYOD) policies. However, organizations that implement strict security policies, such as enforcing endpoint protection and zero-trust architecture, can mitigate risks associated with BYOD while maintaining operational flexibility. This combination of layered technical controls and clearly defined usage policies enables organizations to preserve the productivity gains of remote and hybrid work arrangements while containing the elevated risk that BYOD environments introduce.

Chapter Three

Methodology

Introduction

The purpose of this qualitative research study was to explore cybersecurity strategies employed by small business leaders to protect their businesses from cyberattacks in the post-COVID-19 environment. The study's population included small business leaders from the Seattle metropolitan area. This chapter contains in-depth information about research methodology and instrumentation. First, a summary of the research design and rationale will be presented. Following that, the researcher's potential biases and other ethical issues will be identified, along with plans for dealing with these issues. The research methodology is then discussed, including the process for selecting the target population, sampling procedure, treatment, instrumentation, quality of evidence, data collection procedures, and a data analysis plan. Additionally, ethical procedures, such as Institutional Review Board (IRB) documentation and the protection of human participants, will be discussed. Discussions about reliability and validity will follow, and the section concludes with a transition and summary.

Research Design

The qualitative study method was the most appropriate for this study, as it allowed for an in-depth exploration of effective strategies used by small business leaders to deter cyberattacks in a post-COVID-19 environment. The research question, requirements, and objectives suggested by Khan (2014) served as the foundation for selecting the research method and design for this study. The qualitative method was most appropriate as it aligns with the research goal of investigating strategies implemented by small business owners to assess computer and network security vulnerabilities and prevent security exploitations

(Nguyen & Carter, 2023). Small businesses, particularly in the retail and service industries face increased cyber threats due to limited resources and expertise, making qualitative insights essential for developing tailored cybersecurity strategies (Benson et al., 2024).

Bias

In qualitative research, the researcher is actively involved in both data collection and interpretation, contrasting with quantitative research, where the researcher's role is minimized, and the focus shifts to the processes and data (Denzin & Lincoln, 2023). As a qualitative researcher, the role involves selecting participants and conducting interviews to gather data on the study problem (Braun & Clarke, 2023). The researcher is the instrument for the creation, administration, and validation of interview questions, playing an integral role in the research process (Pezalla et al., 2012). As the sole researcher responsible for data collection in this qualitative study, the researcher serves as the primary data collection instrument. The researcher received a master's degree in economics from Oregon State University in 2009 and relocated to the Seattle metropolitan area after completing his studies. Additionally, the researcher earned a postgraduate diploma in cybersecurity. In October 2024, the researcher published a paper titled *Enhancing Employee Cybersecurity Awareness in Small Businesses* in a peer-reviewed journal. Given the researcher's background in economics and expertise in cybersecurity, the researcher is well-versed in the topic of cybersecurity measures aimed at improving protection against cyberattacks.

The researcher had no prior experience with the small businesses in the research population and had never contacted the participants before this study. The researcher maintained an unbiased stance toward these companies, ensuring objectivity in the research process (Smith & Johnson, 2023). The researcher was solely responsible for creating the

research instrumentation and reaching out to participants to conduct the semi-structured interviews. Participants were provided with a phone number to contact the researcher if they have questions or need clarification regarding the study (Williams & Taylor, 2024). However, the data was collected exclusively through semi-structured face-to-face interviews or Zoom meetings. This method allowed for richer, more detailed insights as the researcher can engage directly with participants in real time, which enhanced the depth and context of the responses (Chen & Zhang, 2023). This approach also ensured transparency and helps minimize any potential biases in the data collection process.

Using the interview protocol allowed the researcher to gain a thorough understanding of the research topic. The researcher conducted semi-structured face-to-face interviews or Zoom meetings with participants to allow them to freely explain cybersecurity issues and incidents in their organization. Interview protocols, according to Anderson and Johnson (2022), were essential when using the interview method because they guided the researcher in collecting consistent and reliable data. The researcher followed the interview protocol (see Appendix A) to ensure consistency during the interview process. During the interviews, the researcher encouraged the participants to speak openly and completely to ensure that their perspective is represented. Furthermore, the researcher remained neutral so as not to influence the participants' responses, which was vital for the validity of qualitative research (Martin & Bell, 2023).

Sample

The sample for this qualitative research study consisted of small business leaders in U.S.-based small businesses in the Seattle metropolitan area. It was anticipated that 10–15 participants would take part in the study. However, sampling continued until data saturation

took place. A nonrandom sampling strategy that facilitated the deliberate selection of participants who have the information, experiences, and skills necessary for the study is known as a purposeful sample (Yin, 2018). To answer the study questions, the researcher used a purposeful sample as one of the most widely used sampling techniques for qualitative research (Chandani et al., 2017; Etikan et al., 2016); initial participants may offer contact information for new participants who satisfy the purposeful sampling requirements. The strategy for gaining access to potential participants involved applying a purposive sample of small business leaders selected from the list of names and email addresses provided by the US Small Business Administration's Western district office. As a result, the study population consisted of participants who meet the study's inclusion criteria and who oversee the cybersecurity policies inside their businesses. Using the purposive sampling method, the researcher did exclude participants who did not satisfy the eligibility criteria. Snowball sampling was used if there were not enough participants.

Inclusion Criteria

Before they took part in the study, participants must meet the following inclusion criteria: (a) have been operating in the Seattle metropolitan area for at least three years; (b) employed less than 500 people; (c) used technology to conduct business; and (d) participated in the business's cybersecurity decision-making process and may or may not have successfully implemented data security measures. Based on their level of familiarity and experience with overarching research questions, the study population was chosen (El-Masri, 2017; Malterud et al., 2016).

Exclusion Criteria

The study excluded small businesses that planned to move out of the metropolitan Seattle area. The study population was chosen based on their location within the specified area. Additionally, small businesses planned to expand and hire more than 500 employees were excluded from the study. This ensured that the research focuses on small businesses within a specific geographical area that were stable in size and are not undergoing significant changes in their operations.

Recruitment

From the population of small business leaders in the Seattle metropolitan region, the researcher used purposive sampling to select 10–15 participants for semi-structured interviews from the list of names and email addresses provided by the US Small Business Administration's Western district office. The researcher chose the first 10-15 participants who met the study's selection criteria. If an adequate number of participants were not reached, snowball sampling would be employed to expand the participant pool. Furthermore, the researcher attended locally organized small business meetings in the Seattle metropolitan area to gain support and accreditation for the study. The researcher also explained how these local meetings can help build awareness of the research and strengthen ties with the small business community.

To ensure that my emails do not end up in participants' spam or junk folders, the researcher used a professional email address associated with my academic institution. The researcher crafted a clear subject line, used a personalized greeting, and included a professional email signature with my full name, title, contact information, and institutional affiliation. The researcher explained the study's purpose, how participants were chosen, and

how their data would be protected. This level of transparency helped participants understand that the email was not a scam or an attempt to access their networks with malicious intent.

To further build trust, the attached a consent form or participant information sheet that outlines my credentials, details the study, and included contact information for questions or concerns. Additionally, the researcher attended local Small Business Development Center (SBDC) meetings or similar events. This not only allowed the researcher to build connections within the small business community but also strengthened the credibility and increased participants' willingness to engage in the study.

The four primary requirements for conducting research with human subjects are gaining informed consent from participants, protecting them from physical, psychological, social, and economic harm, safeguarding their privacy and that of the organization, and ensuring confidentiality (Yin, 2014). The researcher obtained permission from the IRB before beginning data collection. Following IRB approval (see Appendix E), the data collection process begins. Participants were given informed consent forms via Qualtrics to review and complete (see Appendix D).

Instrumentation

Collecting data that can provide a rich, contextual understanding of the research topic in qualitative designs is preferable. The instrument's questions must provide data to help explain the research questions and, ultimately, the research problem (Leedy & Ormrod, 2016). This study's instrumentation was based on a series of researcher-developed interview questions (see Appendix A), which were based on TLT and the NIST CSF.

Semi-structured interview questions provided specific objectives while allowing for clarification and in-depth examination of standout responses. The researcher was able to

establish a connection with participants, creating a comfortable and open environment for sharing information. Semi-structured interview questions included a series of demographic questions as well as the interview protocol. See Appendix A for the actual interview questions that were asked. The demographic and semi-structured interview questions were evaluated using a pilot test with a sample size of two, also known as a pretest.

The pilot test was conducted to ensure that the demographic and interview questions are clear, understandable, and relevant to participants. To enhance the validity of the questions, the interview protocol was reviewed for content and face validity through a Delphi approach, involving a panel of experts in cybersecurity and small business practices. This panel consisted of professionals and scholars in the field who could provide feedback on the clarity, appropriateness, and comprehensiveness of the interview questions. The use of a Delphi approach was preferable, as it drew on multiple expert perspectives, offering a more rigorous validation process compared to relying on a single reviewer, such as a university professor.

Pilot Study

A pilot study identified or refined a research question, determined which methods are best for pursuing it, and estimate how much time and resources was required to complete the larger version (Crossman, 2019). After receiving approval from the IRB, the researcher conducted a pilot study. Like a feasibility study, the pilot study permitted the researcher to execute the planned interview process, evaluate the responses and data collected, and identify any issues or concerns with the structure or setup (Aziz & Khan, 2020).

The researcher conducted a pilot study with two participants from the research population to enhance the validity of the research questions. The researcher selected the pilot

study participants, but the main study would not incorporate their responses. In this pilot study, semi-structured interview questions were conducted for two test participants. The questions were asked exactly as they were written. The pilot study results were used to verify the quality of the interview questions. The researcher for this study used participants' comments from the pilot study to update the interview questions. As a result of the pilot study, changes to the instrument were made to improve the organization of the information flow.

Data Collection Procedures

The research design approach that best addressed the research questions determines the data collection techniques (Yin, 2018). The most common sources of valuable data in qualitative study were participant interviews, accessible documentation, and physical artifacts (Nyumba et al., 2018). The researcher obtained permission from the IRB at Marywood University (MU) before beginning data collection (see Appendix E). Following IRB approval, the data collection process began. Participants were provided with a link to a secure online platform, Qualtrics, where they could review the full informed consent document. After reading the document in its entirety, participants indicated their voluntary agreement to participate by selecting a consent checkbox prior to proceeding with the study. The consent form included a thorough explanation of the study's purpose, benefits, potential risks, the confidentiality of participant data, the right to withdraw at any time, and other ethical considerations (Creswell & Creswell, 2022). The form ensured participants are fully informed about their participation, and they would not proceed with the study until consent was obtained (see Appendix D). Data collection procedure is described in Table 3.

Table 3.

Data Collection and Analysis Timeline

Data Collection and Analysis Procedure
1. Submit the IRB proposal for review and await the IRB approval. 2. IRB Approval Granted (see Appendix E) 3. Upon retrieval of email addresses from SBA, informed consent forms were emailed, utilizing MU's email to participants requesting their willingness to participate in the study. Participants were provided informed consent through an online form (e.g., in Google Forms or Qualtrics), where they could indicate their consent by checking a box that confirms they have read and agreed to the study's terms. 4. Once participants agreed to take part in the study, a pilot study was conducted to assess the validity of interview questions. 5. After a pilot study, invitations were emailed to potential candidates. 6. Semi-structured face-to-face interviews or Zoom meetings were scheduled for a sample of interested participants and were conducted using an interview protocol. 7. Data was coded, and recordings were transcribed. 8. Member checking occurred [participants will confirm the transcripts] 9. Follow up to provide copies of interpretations and finalize member checking. 10. The data was analyzed via thematic analysis. 11. Reported results and findings

The researcher utilized a Sony ICD-PX333 digital voice recorder to document the interviews. The recorded audio files were securely transferred to a password-protected storage device to prevent unauthorized access. To ensure confidentiality, all recorded data were securely stored and would be permanently deleted three years after the study's completion. After this period, the researcher will shred any physical documents and erase all electronic data using KillDisk software to ensure complete data destruction.

After all questions were answered and the participants had no more information to add, the researcher ended the interviews. The researcher concluded the interview with a statement thanking the participants for their time and participation. The researcher transcribed the audio files using Google's Voice Typing function. Participants were contacted via email using a participant confirmation letter (see Appendix C) within one week of the transcribed copy of the researcher's notes to ensure that their responses are accurately captured. At that point, the participants would review the transcribed data from the interview.

To ensure participant confidentiality and minimize the risk of data breaches, transcribed copies of interview responses were not shared via email. Instead, participants received access to their transcripts through a secure, encrypted file-sharing platform via Google Drive. Each participant received a unique, time-limited access link and a separate password to prevent unauthorized access. Participants would then have three business days to review the transcribed data from the interview and provide any necessary corrections or clarifications.

Participants were informed about the importance of accessing the files through a secure connection and encouraged not to download or share the transcript with others. This

method aligned with ethical standards for data protection and complied with the IRB guidelines concerning digital data handling.

Analysis of Data

The researcher analyzed the data after all the information had been checked for accuracy and transcription. The benefits of semi-structured face-to-face interviews or Zoom meetings were much greater than the risks of bias that are recognized and dealt with during the research process. The main data analysis method for this study was thematic analysis. Mackieson et al. (2019) define thematic analysis as requiring the researcher to make intellectual contributions while evaluating data to identify patterns or themes. Thematic analysis helps researchers interpret raw data by identifying codes and themes (Yin, 2018). The thematic analysis involves six steps, according to Neuendorf (2018): familiarizing oneself with the data, generating codes for categories, scanning for themes, reviewing themes, defining and labeling themes, and providing a report. Microsoft Excel (https://www.microsoft.com) would manually code and organize the data by participant code and semi-structured interview questions before data analysis. Participants received unique codes. This study will employ Participant 1=P1 coding. Participant 1 will receive P1 manually. Participants 2, etc., will receive P2 manually. All 11 participants will use this coding method. Many Excel worksheets were prepared to organize and analyze the 11 participants' data sets. Each semi-structured interview question did have its worksheet with participant codes and answers.

After each interview and participant confirmation, the audio files were transcribed using Google's Voice Typing function. The interviews were then reviewed, and any inaccuracies from the Google Voice Typing feature will be manually fixed. NVivo, a

computer-assisted qualitative data analysis software (CAQDAS), was used in the data analysis process. The NVivo software included features for automating and analyzing data generated by various inputs. The NVivo software did not automatically code data into themes but allowed the researcher to visualize the data and identify common themes (Edwards-Jones, 2014). The coding of the themes allowed each participant's similar experiences to be discovered (Leedy & Ormrod, 2015). The researcher categorizes and codes key ideas in the responses after transcribing the interviews, and the researcher established themes from the interview data using NVivo software.

The researcher then compared the findings to the theoretical framework and literature and identify key themes that represented the study's findings. By analyzing the data collected, the researcher could gain insights into the specific cybersecurity strategies small business leaders implement. This analysis provided a comprehensive understanding of the measures taken to safeguard against cyberattacks and contribute to existing knowledge in the field of cybersecurity for small businesses.

Quality of Evidence

In qualitative studies, the validity and reliability of the data collection instrument are crucial for minimizing bias and subjectivity. A qualitative study's validity can be demonstrated by another researcher who reaches the same conclusion using the same data collection method. To ensure the reliability of this study, it meticulously documented all research steps and procedures and ensured that the research methodology and design remain consistent throughout. According to Creswell & Creswell (2022), a qualitative study aimed to provide comprehensive and in-depth information about a particular occurrence. They noted that in qualitative research, validity, reliability, and trustworthiness metrics include some of

the numerous variables considered in developing the research strategy, which will be discussed here.

Validity

Elo et al. (2014) defines validity as the correctness of the findings made by the researcher and participants. Reliability refers to the extent to which a test or any measuring procedure produces the same results on repeated tests under the same conditions. To be considered valid, the measures of the results must be reliable. You can also cite previous research to bolster the validity and reliability of the findings. The researcher can use credibility, transferability, dependability, and confirmability to ensure that the data is trustworthy and free of bias.

To obtain validity, the open-ended questions were designed to elicit behavioral responses from small business leaders. In addition, the researcher compared the construct validity of the identified themes from the data to the purpose of the study. Member checking was utilized to achieve internal validity. The participants inspected the temporary results for accuracy and confirmation of their responses. External validity measured the findings' generalizability concerning other studies (Yin, 2018). Purposive sampling gathered knowledge-rich data relevant to the study's objectives, and a sample of 10–15 participants will be selected from the initial sample for greater external validity.

Reliability

According to Pozzebon and Rodriguez (2014), reliability is the degree to which another researcher can duplicate and replicate the study results. According to Grossoehme (2014), the researcher meticulously documented all stages of data collection, analysis, and interpretation in a journal. The researcher used an interview protocol to ensure that each

question is relevant to the central research question. Participants reviewed responses to the semi-structured interviews to establish member verification as part of the transcription review. To make the results more reliable, as Yin (2018) suggested, participant-specific cybersecurity strategies for small businesses were looked at for methodological triangulation. The researcher also tested the instrument's flexibility and responsiveness to each interview question through a pilot study. Researchers attained reliability when they discovered that comparable patterns would emerge given the same data.

Trustworthiness

In qualitative research, trustworthiness fosters confidence and credibility in the study (El Hussein et al., 2015). In the research process, trustworthiness involves transferability, confirmability, and credibility. Transferability occurs when a researcher applies the findings from one study to another, assuming the results will be similar. First, the researcher encoded the data for confidentiality per Lancaster's recommendations (2017). The NVivo software allowed the researchers to code the data and connected the codes to identify themes (Pokorny et al., 2018). All data, both hard copy and electronic, will be retained by the researcher for three years; after that period, soft copy documents (encoded copies, e-copies, and cloud documents) will be deleted, and all hard copy documents will be destroyed.

Second, member checking improved the truthfulness and accuracy of the collected data which serves as a participant validation technique in which data or results are returned to the participant for verification (Birt et al., 2016). To meet member checking requirements, the researcher transcribed the audio-recorded data collected and distributed a summary to each participant to review and provide feedback on data accuracy to avoid misrepresentation of the information collected.

Chapter Four

Results

Introduction

This qualitative research study aimed to explore cybersecurity strategies employed by small business leaders to protect their businesses from cyberattacks in the post-COVID-19 environment. After obtaining approval from the IRB, the researcher recruited participants from the US Small Business Administration's publicly accessible database where semi structured interviews were conducted with 11 small businesses in the Pacific Northwest area, specifically in Seattle Metropolitan Area. Using an interview protocol allowed the researcher to ensure consistency during the interview process. The data collection process included validating and triangulating data gathered via member checking. All interviews were transcribed verbatim and de-identified to protect participant confidentiality. De-identified transcripts are stored in a secure, access-controlled repository and are available upon request.

Before beginning data collection, the demographic and semi structured interview questions were assessed using a pilot test with a sample size of two participants, but their responses were not incorporated into the main study. Following the pilot test, a few minor adjustments were made. Interviews were conducted in a semi structured format via Zoom, and Google Meet. All participants responded to every interview question to ensure consistency. Each small business leader’s participation in this study was voluntary. Business leaders expressed their willingness to participate in the study by responding with “I consent” to informed consent form via Qualtrics. All participants had the opportunity to ask questions about the research prior to the interviews. The interviews lasted an average of 30-45 minutes, and all participants gave their consent to an audio recording.

To meet member checking requirements, the researcher transcribed the audio-recorded data and shared it with each participant for their review and feedback on the accuracy of the interpretation of their responses, thus avoiding any potential misrepresentation of the collected information (Fields, 2022). This research employed NVivo 15, a computer-assisted qualitative data analysis software (CAQDAS), which was used for classifying and analyzing the data. The NVivo software allows the researcher to code the data and connect the codes to identify themes (Alam, 2020). NVivo accommodates a broader range of data formats compared to ATLAS and MAXQDA, including PDF files, audio files, Word documents, Excel spreadsheets, and others (Simpson, 2024).

After loading the raw data into NVivo 15, the data was systematically categorized and organized using charts to effectively visualize the information. The data from each small business leader's interview was then analyzed using a thematic analysis approach to identify the emerging themes and recurring patterns throughout their interviews and to establish the major themes to capture the insightful information.

The use of grouping techniques helped me to spot emergent data themes NVivo 15 streamlines the categorization of diverse data types, such as documents, PDFs, audio, and video, allowing for their organization into thematic groups (Simpson, 2024). Braun and Clarke (2021) explained that in qualitative research, NVivo 15 acts as a tool to effectively carry out thematic analysis by organizing data and identifying themes. The interviews concluded with a summary of key points highlighted by participants, followed by an opportunity for them to raise any specific queries through member checking. To validate the emergent themes, a word search query was performed in NVivo, aligning them with themes from participant transcripts and categorizing coded data according to these emergent themes.

The qualitative results from semi-structured interviews with eleven participants are presented in this section. A comprehensive examination of security procedures and strategic priorities was made possible by the participants' diverse backgrounds, which included business owners, IT managers, cybersecurity consultants, and senior executives. A thorough codebook that categorizes participant responses into major themes and sub-themes across 16 interview questions was developed as part of the rigorous thematic approach that follows the six steps of Braun & Clarke's (2006) for thematic analysis. These findings set the stage for the discussion that follows, where their implications for theory, practice, and policy are thoroughly examined. Several overarching patterns emerge across the questions: the importance of resource constraints, the strategic elevation of cybersecurity from a technical function to a business imperative, and the profound reshaping of the threat landscape by generative AI.

Demographic Details

The findings reflect the diverse realities of small businesses because the 11 participants represented a balanced cross-section of roles, industries, organization sizes, and experience levels. Four of the 11 participants were IT managers or directors, followed by 3 business owners and founders, 3 cybersecurity consultants and managed service providers, and 1 chief technology officer. There was also a significant representation of younger entrepreneurs under the age of 50. The study also found that most participants were within the working-age range, with only a small percentage being over the age of 60. This demographic breakdown suggests that the study attracted a relatively young and active group of participants. Four small business leaders had a bachelor's degree, seven had a master's degree

(including an MBA) (see Table 4 below). Overall, the study found small business leaders' educational backgrounds varied, with the majority having at least a bachelor's degree.

All 11 participants identified as male, with no female participants represented in the study. As discussed in the limitations section, this gender gap occurred despite active and deliberate recruitment efforts targeting female small business leaders and reflects the broader structural underrepresentation of women in cybersecurity and small business leadership roles. Many participants were highly educated, with 7 out of 11 holding a master's degree and 4 out of 11 holding a bachelor's degree. This relatively high educational attainment may partially explain the elevated cybersecurity awareness and strategic sophistication observed across participant responses and should be considered when assessing the generalizability of the findings to the broader small business population, where educational backgrounds vary considerably more widely.

The participant pool reflected a diverse range of leadership roles. 5 out of 11 participants identified as founders or business owners, 4 out of 11 held security-focused roles, and 2 out of 11 were consultants. Participants reported a broad range of experience in small business ownership, with majority of participants - 7 out of 11 - led organizations that had been in operation for between 1 and 10 years, reflecting a predominantly early-to-mid-stage business profile. A smaller subset of participants - 3 out of 11- reported owning a business for more than 20 years, suggesting the inclusion of highly experienced, long-term operators. This range reflects a meaningful mix of perspectives, combining insights from relatively new business leaders who may still be navigating early-stage challenges with those of seasoned business owners who have likely encountered and adapted to multiple economic cycles, technological changes, and evolving market conditions.

Table 4

Participants' Demographics

Demographics	Description	Participants	Percentage
Age	21-30	4	37
	31-40	2	18
	41-50	2	18
	50+	2	18
	Do not disclose	1	9
	Total	**11**	**100**
Gender	Male	11	100
	Female	0	0
	Total	**11**	**100**
Highest Level of Education	Bachelor's	4	37
	Master's	7	63
	Total	**11**	**100**
Current Job Title	Founder/ Owner	5	45
	Security Function	4	37
	Consultant	2	18
	Total	**11**	**100**
Experience in years	3-5	2	18
	6-10	4	37
	10+	5	45
	Total	**11**	**100**
Years the Company in Operation	1-10	7	63
	11-20	1	9
	20+	3	28
	Total	**11**	**100**
Industry	Technical/ IT Consulting	7	64
	Executive Recruiting & Staffing	1	9
	Public Sector	1	9
	Energy Sector	1	9
	Aerospace	1	9
	Total	**11**	**100**
Number of Employees (including owner)	1-10	4	37
	11-20	3	27
	21-100	1	9
	101-500	3	27
	Total	**11**	**100**

This diversity of experience is particularly significant in the cybersecurity context, as it captures how risk perception, security investment priorities, and threat awareness evolve across different stages of business maturity — offering a richer and more nuanced understanding of how small business leaders develop, refine, and sustain their cybersecurity postures over time.

The sample was heavily concentrated in the consulting sector, with 7 out of 11 participants representing consulting firms. The remaining 4 participants were distributed across executive recruiting and staffing, the public sector, the energy sector, and aerospace — with 1 participant from each industry. While this industry diversity adds breadth to the study, the significant concentration of consulting professionals warrants careful consideration when interpreting the findings, as consulting firms may possess higher-than-average cybersecurity awareness and more formalized security practices compared to small businesses in other sectors.

Taken together, the demographic profile reveals a sample that is uniformly male, relatively young, highly educated, and predominantly drawn from the consulting industry. While these characteristics introduce limitations around generalizability — particularly regarding gender representation, industry diversity, and the elevated cybersecurity maturity likely associated with consulting professionals — they also reflect the real-world composition of cybersecurity-engaged small business leaders who were accessible and willing to participate. These demographic patterns should be transparently acknowledged when interpreting the findings and considered carefully in the context of future research designed to achieve broader and more representative sampling across gender, industry, and organizational size.

At the same time, a notable gender disparity was observed in the participant pool, as no female small business leaders were included in the study. This absence is significant and should be carefully considered when interpreting the findings. Active efforts were made during the recruitment process to include female participants. Specifically, female small business leaders were directly contacted and personally encouraged to participate, with explicit acknowledgment that their perspectives and experiences are especially critical and valuable. To further accommodate their schedules and reduce barriers to participation, an extended deadline was granted beyond the standard response window. Despite these deliberate and targeted outreach efforts, no women who met the study's eligibility criteria ultimately volunteered or completed the recruitment process.

Although the field of cybersecurity has historically been male dominated (Asiry, 2024), excluding female perspectives limits the diversity of experiences and viewpoints captured in the research. This gender disparity is rooted in systemic barriers, including limited STEM exposure for girls in early education (Merayo & Ayuso, 2022), biased recruitment practices that unintentionally discourage female applicants as job postings often use language that is coded as masculine (Moghaddam et al., 2021), and organizational cultures within the cybersecurity industry that often feel unwelcoming to women (Montañez et al., 2020). Future research should prioritize deliberate recruitment strategies to ensure greater gender representation and a more comprehensive understanding of the cybersecurity challenges faced by small business leaders across diverse demographics.

Thematic Analysis

The results of the thematic analysis indicated the presence of 9 major themes that collectively describe how small business leaders approach cybersecurity in the post-COVID-

19 environment. These themes capture perspectives across strategy, operations, human factors, and emerging risks. Table 5 presents the themes that emerged in relation to the corresponding interview questions. The findings indicate a consistent pattern across participants, highlighting both common challenges and shared priorities in small business cybersecurity. The findings also highlighted challenges related to resource and expertise constraints, which often limit cybersecurity investments and capabilities.

Once no new information was obtained from additional participants, I concluded that data saturation had been reached. Saturation was determined through an ongoing process of thematic monitoring conducted concurrently with data collection, whereby newly generated codes and emerging themes were systematically compared to those identified in all preceding interviews after each session. This study experienced data saturation at the eighth interview, at which point no new codes emerged from the data and all themes and subthemes had already been established in prior interviews. The three interviews conducted beyond that point served solely to confirm and reinforce the stability of the identified themes, providing additional confidence in the robustness and transferability of the findings.

Following the identification of these themes, each is presented and described to provide deeper insight into how small businesses conceptualize and implement cybersecurity practices. Due to the large volume of participant responses and codes generated during the analysis, this study focuses on the major themes that emerged most prominently across participant interviews. Consistent with the purpose of Chapter 4, the findings are presented through thematic analysis and supported by representative participant quotations under each theme. Chapter 5 explores the alignment of the study's findings with the theoretical

frameworks, discusses the significance and implications of the results, and offers recommendations for practice, policy, and future research.

Table 5

Major Themes Identified Through Thematic Analysis

Interview Question	Themes	Major Themes
8	1	Foundational Importance of Cybersecurity
9	2	Core Cybersecurity Strategies
10	3	Resource & Expertise Constraints
12	4	Role of Written Cybersecurity Policies
13	5	Securing the Distributed Workforce
14-15, 18	6	Policy Communication, Enforcement and Leadership Role
16-17	7	Training Modalities & Effectiveness
19-20	8	Recovery Planning and Role of Cyber Insurance
11, 21-23	9	Key Emerging Threats & Strategic Advice for Small Business Leaders

Theme 1: Foundational Importance of Cybersecurity

Across all interviews, cybersecurity was consistently highlighted as a critical need for businesses, especially in sectors handling sensitive data, such as healthcare, finance, and government contracts. Ten participants mentioned operational criticality in which the participants referred to the widening attack surface because of remote work, and the increased susceptibility of small businesses. Participants emphasized that cybersecurity has become an operational necessity rather than an optional investment, particularly in the post-COVID-19

environment. One participant explained that the rapid adoption of cloud services, remote work, and SaaS platforms has significantly expanded the attack surface, exposing small businesses to risks that were previously more common among larger enterprises. As noted, “Cybersecurity is no longer optional — it is operationally critical. Post-COVID accelerated cloud adoption, remote work, SaaS reliance, and digital workflows. This significantly expanded the attack surface. Small businesses are now exposed to risks that previously mainly impacted larger enterprises” (P09).

This heightened exposure has also made small businesses increasingly attractive targets for cybercriminals. Another participant highlighted that attackers deliberately focus on smaller firms due to their typically weaker security posture, stating,

> Nowadays attackers are really targeting small business because they know that they don't normally implement a good cyber program. So having that in place will help to mitigate any cyber attackers if you're a victim of a cyberattack, you lose so much money (P02).

Together, these perspectives underscore a critical shift: small businesses are no longer peripheral targets but central players in the evolving threat landscape, requiring deliberate and proactive cybersecurity strategies to mitigate growing risks.

Participants acknowledged that while cybersecurity is universally important, the level of protection implemented often depends on organizational resources, particularly budget and size. One participant noted that without even a baseline level of protection, businesses become easy targets for attackers, emphasizing that investment in cybersecurity varies based on what organizations are willing and able to allocate. As P01 explained,

> If you don't, then you are basically very easily targeted… you need to have at least some level of protection. Some organizations aim for a high level of security, while others do less, depending on their size and how much they are willing to invest.

This resource-dependent approach is further complicated by structural changes in the modern work environment. One participant observed that the shift to remote and hybrid work has effectively dissolved traditional network perimeters, placing critical organizational data in decentralized and more vulnerable environments. As noted, “In the post-COVID-19 landscape… the transition to ‘work from anywhere’ has dissolved the traditional network perimeter, moving the ‘crown jewels’ into a more exposed environment” (P11).

At the same time, participants emphasized a broader strategic shift in how cybersecurity is perceived. Rather than being viewed solely as a defensive IT cost, it is increasingly recognized as a business enabler. One participant highlighted this evolution, stating, “Cybersecurity is a strategic function for organizations of all sizes… it is no longer just about risk reduction—it has become a critical driver of business enablement” (P03).

Together, these insights illustrate a dual reality: while cybersecurity is now a foundational business requirement, the ability to implement robust protections remains closely tied to available resources, making strategic prioritization essential for small businesses operating in an increasingly decentralized threat landscape.

Theme 2: Core Cybersecurity Strategies

Respondents identified a set of critical security controls that together form a multi-layered defense framework essential for protecting small businesses. Among these, MFA emerged as the most widely emphasized control, mentioned by half of the participants. One participant highlighted its importance by noting that the absence of MFA across platforms

significantly increases the attack surface, stating, “you run into a lot of issues when you have local accounts or every single platform with no MFA… your attack surface unnecessarily rose significantly higher” (P08). Another participant reinforced this point more precisely, recommending “MFA everywhere (email, VPN, SaaS, admin accounts)” (P09).

Strong password practices were also identified as foundational control. Participants stressed the importance of complexity and length, with one recommending passwords of at least 15 characters incorporating upper- and lower-case letters, numbers, and special characters to strengthen overall account security (P01). Beyond these baseline controls, participants emphasized the value of adopting broader security frameworks such as zero-trust architecture. One participant noted that zero trust can be particularly effective for small organizations when properly implemented, especially when combined with identity-based controls like MFA (P03). This reflects a shift toward continuously verifying access rather than relying on traditional perimeter-based defenses.

Ongoing monitoring and system visibility were also highlighted as essential practices. One participant stressed the importance of continuously reviewing systems and maintaining awareness through monitoring and regular internal discussions revolving around cybersecurity posture (P02). Complementing this, another participant emphasized the role of detection and response capabilities, noting that even basic monitoring solutions—such as a SIEM or managed detection service—can enable early identification of threats and prevent prolonged undetected breaches. The same participant underscored the importance of preparedness, stating that having an incident response plan in place before an event occurs is critical to avoiding confusion and delays during a crisis (P10). Overall, the findings underscore that effective cybersecurity for small businesses relies on layered controls that combine identity

protection, strong authentication practices, continuous monitoring, and proactive incident response planning.

Theme 3: Resource & Expertise Constraints

There was broad agreement that resource constraints represent the most significant barrier. Decisions around whether to outsource cybersecurity functions, along with concerns about cost and available expertise, were among the most frequently debated issues. Seven participants identified cost and limited resources as the primary challenge for small businesses, while six participants emphasized that a lack of cybersecurity expertise is also a major constraint. The majority of participants (60%) identified cost as the primary obstacle. Participants emphasized that securing stakeholder buy-in remains particularly challenging, as decision-makers often focus on immediate financial implications rather than long-term risk. As one participant explained,

> For a small business, the challenges are, first, getting the stakeholder. When you talk to them and say you need cybersecurity protections, they often ask why, because they are focused on the dollar amount and don't always recognize the risk involved (P01).

In addition to cost, resource limitations were consistently highlighted. Participants noted that small businesses struggle not only with financial constraints but also with limited personnel and capacity to effectively manage cybersecurity. One participant summarized this challenge, stating, "Cost is one of the main issues, but resources overall are also a challenge. Small businesses often don't have the people or the capacity to manage everything that is required for cybersecurity" (P02). Several participants also stressed the consequences of underinvestment, emphasizing the importance of framing cybersecurity in terms of business risk. As one participant noted, "If you don't invest, for example, $10,000 now, a breach could

cost you much more later. It's about helping stakeholders understand the potential financial impact and whether they are willing to take that risk" (P01).

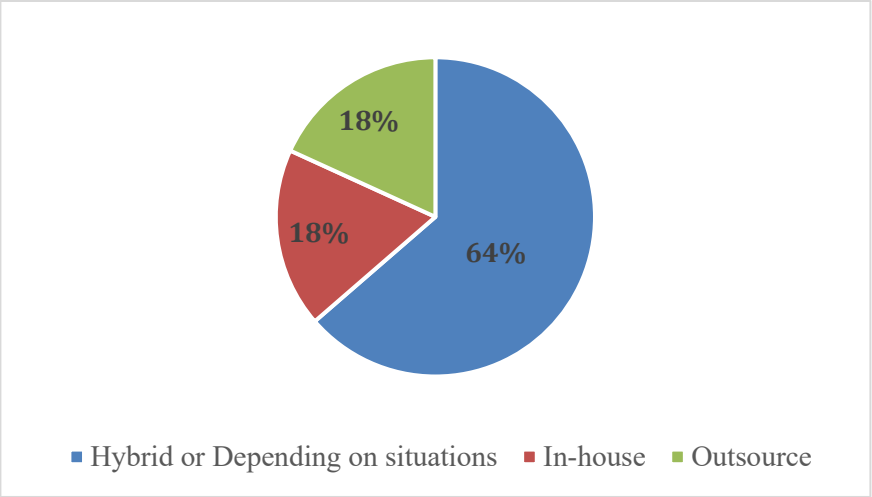
P5 identified budget constraints and a lack of internal expertise as the most prominent obstacles. Another participant expanded on this perspective by highlighting broader workforce challenges, noting, "For small businesses, the primary hurdles are financial constraints and the global talent shortage, which make it difficult to afford and retain specialized staff" (P11). The discussion around maintaining an in-house team versus outsourcing cybersecurity functions revealed differing perspectives; however, 64% of respondents favored a hybrid approach (see Fig. 5). Participants suggested that combining internal oversight with external expertise provides a more practical solution. As one participant stated, "I think the hybrid solution is the best right now, especially as organizations are still trying to determine the most effective approach" (P02). Another participant reinforced this view by emphasizing both the limitations of a fully in-house model and the benefits of outsourcing. As noted, "For most small businesses, a fully in-house team isn't realistic. Outsourcing provides access to expertise and tools that would otherwise be unaffordable" (P10).

Participants emphasized the need for systematic approaches to address cybersecurity challenges. Several highlighted education as a foundational element, noting that a lack of awareness often leads to underinvestment and increased long-term risk. As one participant explained, "The biggest challenge is education… if you don't invest now, you'll pay later in the event of a breach. You also risk losing customer trust, which is difficult to recover" (P08). Others proposed structured, continuous improvement methodologies to strengthen cybersecurity practices. One participant recommended adopting a cyclical framework, stating,

"You can apply the Plan-Do-Check-Act (PDCA) cycle to cybersecurity strategy. It begins with assessing what needs to be done, whether through self-assessment or external evaluation" (P05).

Figure 5

Recommendation for in-house cybersecurity team vs outsourcing



In addition, participants suggested broader structural solutions to improve cybersecurity adoption among small businesses. One participant advocated for integrating cybersecurity into regulatory processes, noting, "Municipalities issuing business licenses could include cybersecurity as part of their compliance checklist. Business owners should also have access to partners or resources to guide them" (P08).

Theme 4: Role of Written Cybersecurity Policies

Many participants agreed that while written cybersecurity policies provide essential structure and consistency, their effectiveness ultimately depends on enforcement and contextual relevance. Policies alone are insufficient unless they are actively integrated into organizational practices and aligned with business needs. Participants described policies as

foundational tools that guide organizational behavior. One participant noted, “Policies serve as documentation that outlines how things should be done and help employees understand expectations and appropriate actions” (P02). Another emphasized their governance role, stating, “Policies create structure, consistency, and accountability by defining expectations and response processes” (P09). Participants also highlighted the practical value of documented procedures, particularly for incident response and preparedness, noting that clearly defined actions improve an organization’s ability to respond effectively to adverse events (P05).

For companies with 20 or less employees, written policies were viewed with notable skepticism regarding their practical value for very small operations. One participant argued that most small business policy work amounts to little more than checkbox compliance: “They just buy a template, they fill it in and they go, we have a policy and it doesn't do anything for them” (P03). This participant acknowledged, however, that policies can serve legitimate purposes — building customer trust and creating genuine contextual awareness of risk — when developed thoughtfully rather than treated as a documentation formality. Another participant suggested that experiential training delivers more practical value than written documentation for very small operations (P07), while a third offered a more affirmative view, noting that even simple policies meaningfully improve decision-making and risk reduction by establishing structure, consistency, and accountability (P09).

Among participants from the largest organizations in the sample — those with 100 to 500 employees — policies were viewed as necessary but fundamentally insufficient without robust technical enforcement mechanisms. One participant challenged the assumption that written policies reliably change behavior: “Your policy is only as good as your ability to

enforce it, to monitor it, if people are actually following it" (P08), illustrating this point with an analogy comparing unenforceable policies to speed limits without traffic enforcement. Participants from larger organizations also emphasized the regulatory and accountability dimensions of written policies, with one noting their critical role in demonstrating due diligence to regulators, insurers, and customers following a breach (P10). The most expansive view came from a participant who described written policies as the operational mechanism through which abstract frameworks such as Zero Trust are translated into enforceable human behavior across a distributed workforce, ultimately transforming security from a series of disconnected tools into a cohesive organizational culture (P11).

Participants underscored the gap between policy creation and enforcement. One participant remarked, "Anyone can write a policy, but without enforcement, it becomes ineffective and can easily be ignored" (P08). Similarly, another participant noted that while policies may provide a level of protection, they do not eliminate risk unless supported by enforcement mechanisms and accountability structures (P08). Participants further emphasized that policies should be embedded within broader strategic planning, including risk tolerance and long-term organizational objectives, to ensure meaningful impact (P05).

Participants highlighted that policies must go beyond documentation to foster understanding and behavioral change. One participant observed, "Policies are only valuable if they create contextual awareness and help organizations address the risks that matter most" (P03). Another participant suggested that, particularly for small businesses, training and awareness initiatives may be more effective than formal documentation alone in promoting security-conscious behavior (P07). Additionally, participants stressed that cybersecurity risks

vary across organizations, and policies must be tailored accordingly to avoid ineffective or misaligned investments (P05).

Overall, participants agreed that while policies serve as essential blueprints, their value depends on enforcement, operational integration, and contextual relevance. Effective cybersecurity policies are not merely documents but part of a broader framework that combines structure, accountability, strategic alignment, and organizational awareness to support meaningful risk mitigation.

Theme 5: Securing the Distributed Workforce

The expansion of remote work and BYOD practices has significantly widened the organizational attack surface. As a result, participants consistently advocated a transition from traditional perimeter-based security toward identity-centric and zero-trust frameworks, where access control follows the user and the data rather than the network boundary. Participants emphasized that BYOD introduces substantial and often unavoidable security challenges. Personal devices, frequently connected to unsecured networks, create exposure points that organizations struggle to monitor and control. As one participant observed, “remote work…using your own device…presents a lot of…security issues…different Wi-Fi…can allow for attackers to target those areas” (P02). This concern is compounded by limited organizational authority over privately owned devices, with another noting that “BYOD is particularly tricky because the organization has limited ability to enforce security standards” (P10).

Participants across all industries acknowledged that remote work and BYOD arrangements significantly expand the attack surface for small businesses, but their concerns, proposed solutions, and tolerance for BYOD risk varied considerably by industry. Among IT

and cybersecurity consulting participants, perspectives ranged from pragmatic acceptance to structured technical mitigation, reflecting the tension between what is theoretically ideal and what is operationally realistic for very small businesses. One participant offered a candid acknowledgment of small business limitations, arguing that BYOD is an unavoidable reality that small businesses largely must accept while offsetting exposure through well-designed cloud environments: “For small businesses, personal devices are a way of life... I don't know any good strategy for a small business on how you manage that risk. I think you largely have to accept it” (P03). Other IT consulting participants were more prescriptive, recommending layered technical controls including VPN, MFA, log auditing, and device segmentation (P01; P02), while the most technically sophisticated response advocated for Zero Trust Network Access combined with endpoint detection and response as the definitive architectural solution: “With Zero Trust network access, we can control the accessibility between the employees and the device to the company's data center or SaaS application” (P04).

The healthcare IT participant offered the most technically advanced solution of all, advocating for virtual desktop infrastructure as the optimal approach to eliminating BYOD risk entirely: “I have a thin client at home that is read only. I can't write to the device and from there all I'm able to do is access my virtual desktop that runs in Azure” (P08). This participant explained that virtual desktops are destroyed and reimaged nightly, creating a near-impenetrable barrier between personal device threats and organizational data, while reducing costs through consolidated licensing and simplified management. Notably, this participant attributed the sophistication of this approach directly to healthcare's regulatory environment and HIPAA compliance obligations — suggesting that regulatory pressure is a

significant driver of BYOD mitigation maturity in ways that extend well beyond general cybersecurity awareness.

The energy sector participant described BYOD as particularly challenging due to the organization's limited ability to enforce security standards on personal devices, recommending a comprehensive policy-and-control hybrid combining VPN, MFA, mobile device management, and containerization to separate work and personal data (P10). The public sector participant offered the most governance-oriented framing, arguing that businesses must shift from physical perimeter-based security toward identity-centric models that protect data regardless of device or location: “Ensuring that the crown jewels remain protected by a security perimeter that follows the data, rather than one tied to a physical office” (P11).

The discussion also highlighted the practical realities faced by smaller organizations, where BYOD is often not optional but necessary due to resource constraints. In such contexts, reliance on employee practices becomes inevitable, reinforcing the human factor in security risk. Participants further underscored the compounded risks of credential reuse, data leakage, and unauthorized access stemming from the convergence of personal and professional use. As one participant metaphorically framed it, investing heavily in securing enterprise infrastructure is undermined if “a personal device…with none of that security [is given] access to all of the crown jewels” (P05). This reflects a broader concern that BYOD can effectively bypass otherwise robust security architectures.

To mitigate these risks, participants identified a suite of foundational security controls. These include the use of secure virtual private networks (VPNs), MFA, endpoint registration, logging, and encryption. One participant summarized that “best practice…[includes]

VPN…strong VPN…[and] multi factor authentication…[along with] verifying…communication…and auditing" (P01). Such measures represent the baseline for securing remote access in distributed environments.

However, participants also stressed that these controls must evolve beyond broad network-level access. Instead, there is a growing emphasis on granular, identity-driven security mechanisms. Strategies such as mobile application management (MAM), containerization, and conditional access policies were highlighted as critical for isolating corporate data and verifying device integrity prior to granting access. As one participant explained, organizations should "move away from broad network access toward identity-centric security…ensuring that the 'crown jewels' remain protected by a security perimeter that follows the data" (P11). This reflects a shift toward contextual and continuous verification models aligned with zero-trust principles. Beyond baseline controls, participants advocated for more transformative approaches to remote access security. A notable trend is the declining reliance on traditional VPN architectures in favor of zero-trust network access (ZTNA) solutions. As one participant stated, they were "less of a fan of…classic VPN…[and] much more interested in a zero-trust model" (P03), highlighting the perceived limitations of legacy approaches.

Virtual desktop infrastructure (VDI) and application virtualization were also strongly endorsed. These solutions centralize computing resources and minimize endpoint risk by restricting data storage and processing to controlled environments. One participant described using a thin client that only accesses a cloud-hosted virtual desktop, noting that such systems are regularly reimaged, making it "very hard for malware to survive" (P08). Similarly, application virtualization was praised for its efficiency and security benefits, allowing

organizations to maintain a single, centrally managed application instance rather than distributing software across multiple endpoints.

In contrast to BYOD, some participants proposed more traditional but effective alternatives, such as issuing company-owned and managed devices. Notably, this perspective came from a participant leading a small technical consulting firm of fewer than 20 employees — an organizational context where the cost of provisioning dedicated work devices remains feasible while the security risks of BYOD are sufficiently tangible to justify the investment. As this participant noted, "a cheaper solution…is to provide devices…[and] not allow personal devices for business transactions" (P06). This finding suggests that for small businesses in technically oriented industries with sufficient staff to warrant device management overhead, company-owned device provisioning may represent a more practical and enforceable alternative to BYOD risk mitigation strategies that rely heavily on employee compliance and behavioral controls. This approach reduces variability and enhances enforceability of security policies, albeit with higher upfront costs.

Overall, there was strong consensus that the evolving nature of work necessitates a paradigm shift in cybersecurity strategy. Traditional perimeter defenses are increasingly inadequate in environments characterized by mobility, cloud adoption, and device heterogeneity. Instead, participants emphasized the importance of adopting identity-centric, zero-trust approaches supported by advanced technologies such as conditional access, virtualization, and centralized control mechanisms. Ultimately, effective security in remote and BYOD contexts depends on repositioning protections around users, devices, and data—rather than fixed network boundaries.

Theme 6: Policy Communication, Enforcement and Leadership Role

Participants consistently emphasized that policy communication must be ongoing, accessible, and practical, rather than episodic or overly formalized. One participant highlighted that "communication has to be ongoing—not just a one-time email…leadership needs to reinforce it…[and] consequences…need to be real" (P10), underscoring the importance of sustained reinforcement and accountability. This aligns with the broader view that policies are only effective when they are actively integrated into daily organizational discourse.

Simplicity and relevance were also identified as critical success factors. As noted, policies should be "simple, practical, repeated, [and] leadership-endorsed," ensuring they remain actionable and visible to employees (P09). Participants stressed that lengthy, complex documents are rarely engaged with in practice; instead, policies must be distilled into digestible and role-relevant formats. One participant observed that "nobody reads a 50-page policy document—simplify it and make it digestible" (P10).

In addition, modern communication strategies were seen as enhancing engagement and retention. Techniques such as micro-learning, simulated phishing exercises, and real-time feedback mechanisms were recommended as more effective alternatives to traditional, infrequent training sessions. Verbal reinforcement, alongside written documentation, was also highlighted as a means of improving retention, particularly when combined with practical "do's and don'ts" guidance embedded into everyday workflows (P02).

A central theme across the data was that policy enforcement should not rely solely on human behavior but must instead be operationalized through technological mechanisms. Participants emphasized the value of integrating policies directly into the IT environment,

thereby transforming them from abstract guidelines into enforceable controls. As one participant explained, enforcement is most effective when "integrated directly into the technology stack…[so] the policy becomes a functional reality rather than just a suggestion" (P11).

Automated enforcement mechanisms—such as conditional access controls, automated policy engines, and security monitoring systems—were widely endorsed. These tools can proactively block or restrict access when predefined conditions (e.g., lack of multi-factor authentication or unpatched devices) are not met, effectively creating "guardrails" that ensure compliance without constant manual oversight. Advanced monitoring capabilities, including data loss prevention, packet analysis, and SIEM integration, were also identified as essential for detecting anomalies such as unauthorized data sharing or exfiltration (P06).

Participants further stressed the importance of embedding enforcement into routine workflows. For instance, real-time prompts or alerts—such as warnings when sending potentially sensitive information—can act as immediate corrective interventions (P07). Additionally, foundational security principles such as role-based access control (RBAC) and segregation of duties were highlighted as critical for limiting excessive privileges and reducing the risk of internal misuse (P01).

While technical controls are essential, participants underscored that policies must be grounded in clear documentation, visibility, and organizational accountability. Policies should be formally documented, easily accessible, and explicitly communicated to all employees. As one participant noted, simply agreeing on policies at the managerial level is insufficient; "employees have to be informed" and know where to find them (P05).

Participants emphasized that employees should feel comfortable reporting mistakes or security incidents without fear of disproportionate punishment. One participant argued that fostering such an environment is "way more valuable than…a set training security awareness course," particularly in smaller organizations (P03). This perspective reflects a shift toward viewing employees not merely as risks, but as active contributors to organizational security. At the same time, accountability mechanisms—including disciplinary actions—were recognized as necessary to reinforce policy adherence. The combination of clear expectations, consistent communication, and enforceable consequences was seen as critical for ensuring that policies are not only understood but also followed in practice (P10).

The findings further underscore the critical role of psychological safety and positive reinforcement in fostering effective security behaviors. Participants converged on the view that employees must feel comfortable in reporting incidents, with leadership playing an active role in shaping a blame-free, trust-based culture. Participants consistently emphasized that removing blame and normalizing incident reporting are foundational to organizational security. As one participant concisely stated, "remove blame, normalize reporting, reward transparency…[employees should see] reporting as part of protecting the business, not admitting failure" (P09). This framing repositions reporting from an act of confession to one of responsibility and contribution.

Leadership tone was identified as the decisive factor in enabling—or inhibiting—such behaviors. One participant noted that when employees fear punishment, "they're not going to report it…they're going to hide it. And hidden incidents are way more dangerous than reported ones" (P10). This highlights a critical risk dynamic: unreported incidents can escalate undetected, amplifying organizational exposure. To mitigate this, participants stressed the

importance of explicitly communicating that mistakes are expected, and that the organizational priority is remediation rather than blame. Mechanisms such as anonymized reporting channels were also suggested to lower psychological barriers to disclosure.

More broadly, participants linked cybersecurity behavior to general organizational culture. Effective environments were described as those where failure is treated as a learning opportunity rather than a liability. As one participant explained, “when failure…[and] lessons learned…are rewarded [employees are] much more likely to report security problems” (P03). Similarly, fostering a culture of “safe risk-taking” was seen as essential; without it, employees may conceal errors due to fear of shame or punitive consequences, thereby increasing overall risk (P07). These insights reinforce that cybersecurity resilience is deeply intertwined with broader leadership practices and cultural norms.

Participants highlighted the importance of positive reinforcement mechanisms that actively encourage secure behaviors. Rather than penalizing mistakes, several participants described how they personally encouraged their own organizations to recognize and reward employees for proactive security actions, such as reporting phishing attempts, flagging suspicious activity, and promptly disclosing potential vulnerabilities. These participant-leaders emphasized that shifting from a punitive to a recognition-based approach helped foster greater employee engagement with cybersecurity practices and reduced the reluctance employees often feel when reporting errors or near-miss incidents. One participant described a simple yet effective strategy: employees who reported suspicious emails received small tokens of appreciation, reinforcing their role in the security process and encouraging continued vigilance (P05).

Training approaches were also discussed in this context, with strong caution against punitive models. Simulated phishing exercises, while valuable, can be counterproductive if framed as tests with negative consequences. As one participant explained, when training is punitive, “they're not going to report other cybersecurity incidents,” whereas supportive approaches that make employees feel valued lead to greater engagement and transparency (P03). This reflects a broader pedagogical shift from compliance-driven training to behavioral reinforcement and participatory learning.

Participants further emphasized that fostering a blame-free culture requires reframing security as a shared organizational responsibility. One respondent noted the need to move from a punitive mindset to “collective vigilance,” where employees are recognized as a critical “human firewall” against increasingly sophisticated threats (P11). In this model, accountability remains important, but it is balanced with encouragement, recognition, and continuous learning.

A central concern raised by participants was the disconnect that can arise when leadership operates outside the constraints imposed on the broader workforce. Such inconsistencies were viewed as highly detrimental to policy legitimacy and organizational trust. As one participant observed, leaders “have to practice what they preach,” noting that policy exceptions for executives—such as bypassing standard device or access controls—undermine the shared security framework and signal that compliance is negotiable (P05). This perceived double standard not only weakens enforcement but also erodes employee motivation to adhere to policies.

Closely related to this is the expectation that leaders act as visible role models. Participants stressed that effective leadership extends beyond enforcement to demonstration,

with one noting that leaders should "be a good example…[not] just enforce something" (P01). This visibility reinforces norms and communicates that security practices are both necessary and universally applicable. The principle that no individual is exempt from policy was repeatedly underscored. Participants pointed to common scenarios in which senior executives receive preferential treatment—such as using personal devices or requesting tailored configurations—as illustrative of systemic risk. As one participant stated, "no one is above policy," emphasizing that such exceptions compromise both security posture and organizational fairness (P08).

Participants highlighted that leadership engagement must be active rather than symbolic, particularly in the context of evolving security paradigms such as zero-trust. One participant explained that when executives visibly adhere to the same controls—such as consistently using MFA and participating in security exercises—they help normalize these practices and reduce resistance among employees. In doing so, leadership reframes security from a technical imposition to a shared organizational value, embedded within everyday operations (P11).

Participants emphasized that leadership behavior has a cascading effect on organizational norms. As one participant noted, when leaders bypass controls for convenience, "that message trickles down fast," whereas visible adherence signals that policies are non-negotiable (P10). This reinforces the idea that leadership actions serve as informal but powerful communication mechanisms, shaping employee attitudes toward compliance. Leadership visibility must extend beyond passive adherence to active advocacy. Participants stressed that leaders should regularly communicate about cybersecurity in meetings and organizational messaging, thereby maintaining its salience and reinforcing its

importance across all levels of the organization (P10). This consistent presence helps integrate security into everyday business discourse rather than isolating it as a technical concern.

A key insight from the data is the necessity of reframing cybersecurity as a strategic business priority rather than an isolated IT function. As one participant explained, organizations take security more seriously when it is positioned as a leadership issue, not merely a technical one (P10). This reframing elevates cybersecurity to the level of organizational governance and risk management, aligning it with broader business objectives.

Closely linked to this is the role of leadership in resource allocation and prioritization. Participants pointed out that without executive buy-in, cybersecurity initiatives are unlikely to receive sufficient funding or organizational support. As one participant precisely stated, if leadership does not recognize its value, "they're not going to promote it…[or] fund it" (P08). This underscores that effective security implementation is contingent not only on technical capability but also on strategic commitment from senior decision-makers.

In addition to strategic oversight, participants highlighted the importance of leaders demonstrating practical cyber hygiene behaviors. Simple, visible actions—such as refusing to share passwords or carefully verifying identities—serve as tangible examples that employees can emulate. As one participant noted, leaders should actively share their own practices, reinforcing expected behaviors through everyday actions (P06).

Furthermore, participants emphasized the value of recognition and positive reinforcement at the organizational level. Leadership can strengthen security culture by celebrating "security champions"—employees who identify and report vulnerabilities or contribute to safer practices. As noted, making security a recurring agenda item in leadership discussions and visibly rewarding such contributions signals that cybersecurity is both valued

and integral to organizational success (P11). The word cloud further reinforces the interdependent relationship between policy, employees, and training in strengthening organizational data protection (see Fig. 6). It illustrates that effective cybersecurity is not achieved through isolated measures, but through the alignment of structured policies, informed employees, and continuous training. Together, these elements create a cohesive security posture in which policies provide direction, training builds awareness, and employees actively contribute to safeguarding organizational assets.

Figure 6

Word Cloud of Policy Communication, Enforcement and Leadership Role

Theme 7: Training Modalities & Effectiveness

Participants emphasized that, in effective training formats, frequency is more critical than duration. Rather than relying on lengthy annual sessions, respondents highlighted the value of shorter, recurring engagements that reinforce awareness over time. As one participant noted, “Organizations that do it well run phishing simulations and frequent awareness nudges.

Annual training gets forgotten quickly, while regular touchpoints keep security top of mind" (P10). Similarly, another participant recommended a structured but recurring approach, stating, "Security awareness training should be conducted at least quarterly to keep the conversation going, while also exploring accessible formats such as online sessions to maintain engagement without excessive cost" (P05). This perspective reflects the need to balance effectiveness with resource constraints, particularly for small businesses.

The importance of delivering training in smaller, more frequent segments was further emphasized by participants who advocated for continuous reinforcement through brief interactions. One participant explained, "I prefer smaller training segments delivered more frequently, short updates in newsletters or periodic reminders help maintain awareness over time" (P03). Another participant supported a blended approach, combining periodic campaigns with formal training, noting that "quarterly phishing campaigns alongside annual formal training provide both consistency and structure" (P08).

Participants emphasized that ongoing interaction and continuous reinforcement are critical components of effective cybersecurity awareness. Rather than treating employees as passive recipients of training, respondents highlighted their role as active participants in organizational defense. As one participant explained, "There should be continuous campaigns and reminders… employees can be the first line of defense, but also the first break in the kill chain, especially in social engineering attacks" (P06).

Person-led training was also identified as particularly impactful. Participants noted that direct, instructor-led engagement creates longer-lasting awareness compared to automated methods. One participant observed, "Person-led security awareness training has a lasting impact… whereas short, automated videos often fail to deliver meaningful learning"

(P05). In addition, approaches such as micro-learning and simulated phishing campaigns were recommended as effective alternatives to traditional models. As one participant noted, "Organizations have moved away from once-a-year training toward continuous micro-learning and simulated phishing, covering modern threats like deepfakes and credential theft" (P11). Practical tools were also highlighted, with one participant describing platforms such as KnowBe4 as enabling organizations to deliver ongoing, accessible training tailored to evolving threats (P01).

Participants strongly criticized annual, compliance-based training. One participant stated, "Most small businesses rely on annual compliance training, which is not very effective on its own" (P10). Others noted that such approaches are often limited to passive, one-time sessions that fail to build lasting awareness. As one participant explained, "Many organizations rely on one-time, lecture-style training because they lack the capacity for more customized approaches, but this rarely leads to meaningful engagement" (P03). The use of phishing simulations without accompanying education was also criticized. One participant argued, "Running phishing campaigns alone is not training… it only measures how susceptible employees are without improving their understanding" (P05).

In terms of training content, tools, and delivery, participants emphasized the importance of practical, actionable learning. Platforms such as KnowBe4 were recommended for delivering structured training programs, while managed service providers were identified as valuable partners in supporting implementation (P08). Participants also stressed that training should include hands-on guidance, with one noting, "Employees need to learn how to identify phishing attempts and understand the steps to report them, not just be shown examples" (P05). Foundational topics such as password hygiene and threat recognition were

considered essential (P09), alongside tools like Wizer that help communicate technical risks in accessible ways (P07). Additionally, participants highlighted the importance of integrating cybersecurity awareness into daily operations, including safe browsing practices, secure access, and clear reporting procedures (P02).

Within the framework of behavioral and performance metrics, participants identified phishing simulation results as the most practical and widely used measure of training effectiveness. These simulations were viewed as a tangible way to assess behavioral change over time. As one participant noted, “Phishing simulation click rates are a practical metric… if fewer employees are clicking over time, it indicates that training is having an impact” (P10). Another participant emphasized the importance of longitudinal tracking, explaining that organizations can monitor progress by observing declining click rates across successive campaigns, noting that while results may improve incrementally, they are unlikely to reach zero (P05).

The concept of the phish-prone percentage (PPP) was also highlighted as a key indicator of susceptibility to phishing attacks. One participant explained, “The Phish-Prone Percentage tracks how many employees click on simulated phishing links, with the goal of reducing this number through consistent training” (P11). In addition to measuring risky behavior, participants stressed the importance of tracking positive security actions. As one participant noted, “Forward-thinking organizations prioritize reporting rates and the speed at which employees flag suspicious activity, viewing increased reporting as a sign of a vigilant workforce” (P11). Similarly, reductions in overall security incidents and risky user actions were identified as indicators of improved cybersecurity posture (P05). Knowledge validation through follow-up assessments was also recommended, with one participant suggesting that

testing employees after training helps determine whether learning outcomes are effectively retained (P01).

In the category of risk, compliance, and process metrics, participants emphasized the importance of structured assessments and alignment with established frameworks. One participant described the use of risk assessments and gap analyses, noting that "frameworks such as NIST are used to evaluate the current state and identify gaps relative to desired security standards" (P02). Participants also highlighted the importance of understanding regulatory requirements, particularly for organizations handling sensitive data, as compliance obligations reinforce the need for cybersecurity measures (P04). At the same time, respondents cautioned against overreliance on compliance-driven approaches. One participant noted that organizations should transition from a "checkbox" mentality to a risk-based strategy that prioritizes protection of critical assets (P11).

Automated monitoring and reporting mechanisms were also identified as valuable tools for tracking training participation and performance. One participant explained that platforms can monitor completion rates, identify individuals requiring additional training, and generate periodic reports to support accountability and continuous improvement (P07). The importance of remediation was further emphasized, with participants noting that employees who fail to meet expectations should undergo repeated training until adequate understanding is achieved (P01). Additionally, metrics such as Mean Time to Detect (MTTD) were highlighted as useful indicators of how quickly human-related threats are identified and addressed (P11).

Under administrative and foundational metrics, participants noted that completion rates alone are insufficient indicators of effectiveness. As one participant observed, "Many

small businesses simply track training completion, but do not evaluate whether behavior is actually changing" (P10). Overall, participants emphasized that meaningful measurement requires a combination of behavioral, performance, and risk-based metrics to accurately assess the impact of cybersecurity awareness initiatives.

Theme 8: Recovery Planning and Role of Cyber Insurance

What distinguished participants' perspectives on recovery planning from standard industry best practices was not simply their awareness of technical tools, but how they conceptualized preparedness, continuity, and recovery as integrated strategic business capabilities essential to organizational survival — rather than isolated IT functions to be delegated to technical staff. Participants articulated recovery not as a checklist of technical procedures but as a leadership responsibility and organizational mindset that must be deliberately cultivated before an incident occurs.

Participants consistently framed recovery planning through the lens of business survivability rather than technical restoration. One participant captured this strategic orientation most concisely: "Preparation determines survivability" (P09). This framing — positioning preparedness as the primary determinant of whether a small business survives a cyber incident — reflects a fundamentally different conceptualization of recovery than the technical-restoration focus that dominates existing cybersecurity frameworks and literature. Rather than asking "how do we restore our systems," participants were asking "how do we ensure our business continues to exist" — a distinction that carries significant implications for how recovery planning guidance is developed and communicated to small business leaders.

Participants reached a consensus that effective recovery from cyber incidents requires a combination of robust backups, well-tested incident response plans, and coordinated

external support. These elements were viewed as mutually reinforcing components of organizational resilience rather than standalone solutions. Within the sub-theme of foundational plans, backups, and processes, participants emphasized that reliable backup strategies and clearly defined response procedures are central to recovery. One participant highlighted the strategic importance of data management, stating, “High-quality backups and a strong data management strategy are critical… in many cases, prioritizing data recovery over infrastructure recovery is more important” (P03). This perspective underscores the need to focus on protecting critical data assets as the primary objective during recovery efforts.

This strategic orientation was further evident in how participants prioritized data recovery over infrastructure recovery. One participant highlighted that in many cases, restoring critical business data is more important than restoring the underlying technical infrastructure: “High-quality backups and a strong data management strategy are critical… in many cases, prioritizing data recovery over infrastructure recovery is more important” (P03). For small businesses operating with fewer than 20 employees and without dedicated IT infrastructure, this insight reflects a pragmatic and resource-conscious understanding of recovery that enterprise-grade frameworks do not adequately address — one that centers on protecting the business assets most critical to continuity rather than replicating complex technical recovery architectures that exceed small business capacity and budget.

Participants emphasized that the effectiveness of recovery planning is determined not by the sophistication of documented procedures but by the degree to which those procedures have been practiced, tested, and internalized by the people responsible for executing them under pressure. Regular tabletop exercises were identified as the critical mechanism through which plans are transformed from paper documents into organizational muscle memory. One

participant noted that such exercises validate communication channels and contingency processes, transforming potentially catastrophic disruptions into manageable events (P11). Another compared incident response preparation directly to routine safety drills, emphasizing that repeated practice is what separates organizations that survive incidents from those that do not (P01). This emphasis on behavioral preparedness over procedural documentation represents a meaningful contribution beyond existing literature, which has tended to focus on the content of recovery plans rather than the organizational learning processes through which small businesses develop genuine response capability.

Participants emphasized that the goal of cybersecurity is not perfection but resilience. One participant succinctly stated that while perfect security is unattainable, consistent and risk-based practices can achieve resilient security (P09). The concept of cyber resilience was further explained as a layered approach that integrates technical controls with organizational culture. One participant explained that resilience requires combining safeguards such as multi-factor authentication and network segmentation with a blame-free culture in which employees actively contribute to security as a human firewall (P11). The focus therefore shifts from preventing every attack to minimizing impact — reducing the "blast radius" through measures such as secure backups, continuous training, and financial safeguards like cyber insurance (P11). Proactive preparedness was identified as essential, with participants advocating for always having incident response capabilities ready to execute (P01).

Participants highlighted the critical role of engaging external stakeholders. One participant explained that organizations should promptly contact legal counsel and insurance providers following an incident to understand obligations and response procedures (P01). The value of cybersecurity insurance was also emphasized, with one participant noting that many

small businesses underestimate its importance until after an incident occurs (P05). Participants further stressed the need to notify vendors and customers when appropriate, particularly to prevent the spread of secondary attacks (P01).

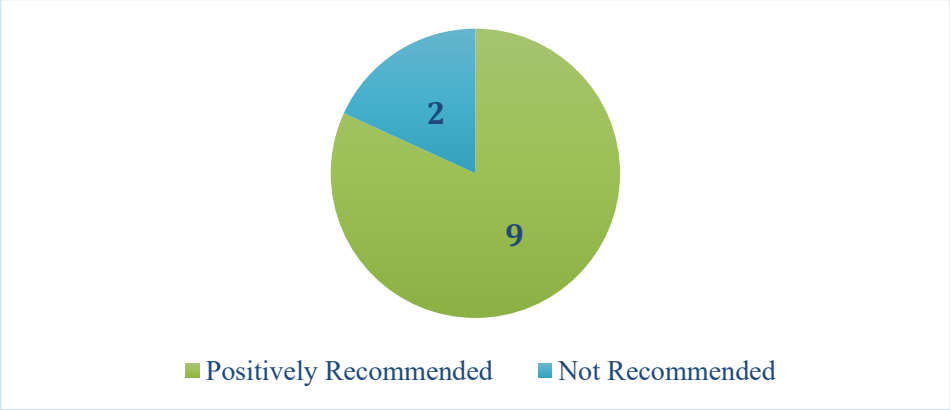
The importance of pre-established relationships with external partners was also highlighted. One participant noted that having prior arrangements with forensic specialists and other partners enables faster and more effective response, particularly when internal expertise is limited (P11). Similarly, another participant emphasized that knowing in advance who to contact—including legal, public relations, and law enforcement—reduces delays and confusion during an incident (P10). The use of cloud-based solutions was also identified as a practical recovery mechanism, with participants noting that cloud providers can support rapid restoration and improve overall resilience (P02). Within proactive, strategic, and operational measures, participants consistently emphasized that preparation is the key determinant of successful recovery. As one participant precisely stated, “Preparation determines survivability” (P09).

Finally, participants highlighted the concept of cyber resilience, defined as the ability to continue operating during an attack. One participant noted that resilience-focused strategies enable organizations to maintain critical functions even under adverse conditions (P11). The use of automated systems was also recommended to support continuous monitoring and response, particularly for small businesses with limited resources (P04). Additionally, participants emphasized the importance of prioritizing core business functions, ensuring that essential services can continue even if other systems are compromised (P05). Overall, the findings suggest that effective incident response and recovery require a holistic approach that integrates planning, coordination, testing, and resilience-focused strategies.

Participants emphasized that cyber insurance serves as a financial backstop and supports incident response efforts. One participant noted, “Cyber insurance helps transfer financial risk and can cover losses when incidents occur, reducing the burden on the organization” (P02). Another participant elaborated on its broader value, explaining that it “transfers the high costs of breaches and provides access to experts such as forensic investigators and legal counsel, strengthening incident response capabilities” (P11). Participants also highlighted its role in mitigating the financial impact of cyber incidents, with one noting that insurance can cover costs such as legal fees, recovery efforts, and ransom negotiations (P10). 9 out of 11 participants recommended purchasing cyber insurance, while 2 out of 11 did not support its adoption (see Fig. 7). This distribution indicates a strong overall endorsement of cyber insurance as a valuable component of risk management, despite some reservations among a small number of respondents.

Figure 7

Recommendation for Cyber Insurance



The importance of cyber insurance as part of a broader risk management strategy was consistently reinforced. One participant observed that “if potential losses exceed available financial resources, cyber insurance becomes a necessity rather than an option” (P11).

Another participant emphasized that while insurance is beneficial, it should be implemented alongside strong foundational controls, noting that it "supports financial risk transfer and recovery but is not a substitute for effective security practices" (P09).

Participants highlighted that insurance requirements can drive improved cybersecurity practices. One participant explained that insurers increasingly require organizations to demonstrate baseline security controls, stating that "organizations must maintain minimum cyber hygiene to obtain and retain coverage" (P07). Additionally, participants noted the potential for insurance providers to play a more proactive role by offering preventative services, which could enhance organizational preparedness and support broader digital transformation efforts (P03). However, a lack of awareness among small businesses was identified as a barrier, with some participants noting that many organizations are unfamiliar with cyber insurance unless they have prior exposure or training (P02).

Under limitations, misconceptions, and risks, participants cautioned against overreliance on cyber insurance. One participant stated, "Cyber insurance is an important part of risk management, but it should not be seen as a replacement for good security practices" (P10). Others noted that insurers are becoming more stringent, requiring evidence of security controls before providing coverage, which may limit access or increase costs for organizations with weak cybersecurity postures (P10). Participants also highlighted that insurance does not address operational disruptions, emphasizing that organizations must still restore systems and resume operations independently (P04).

Finally, participants addressed common misconceptions, particularly the belief that small businesses are too small to require cyber insurance. One participant noted that many organizations underestimate their exposure until after an incident, particularly when handling

sensitive customer data (P05). Overall, the findings suggest that while cyber insurance is a valuable component of a comprehensive risk management strategy, its effectiveness depends on integration with strong security practices, organizational awareness, and realistic expectations of its limitations.

Theme 9: Key Emerging Threats & Strategic Advice for Small Business Leaders

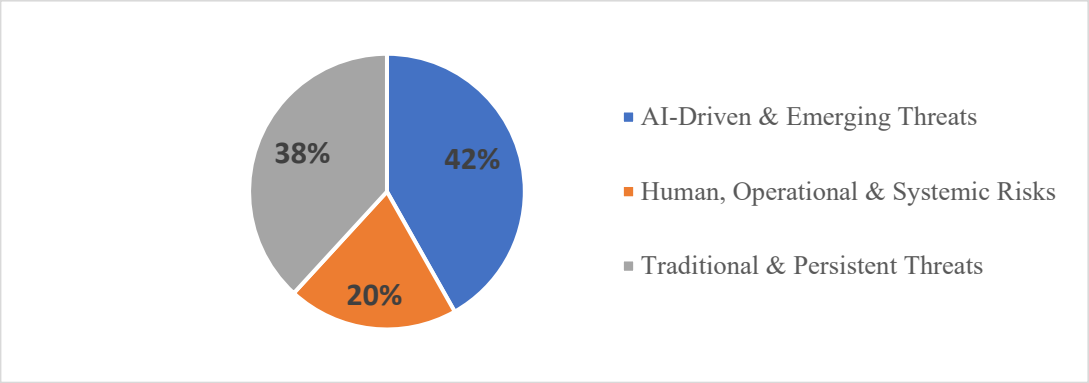
A meaningful pattern emerged across industries in how participants perceived and prioritized emerging threats, revealing that industry context significantly shaped both threat awareness and strategic response. Participants from IT and cybersecurity consulting — the largest industry group with 5 out of 11 participants — demonstrated the broadest and most technically sophisticated threat awareness, consistently identifying AI-driven attacks, supply chain vulnerabilities, identity-based threats, and quantum computing as primary concerns, and articulating structured, architecturally grounded responses. Notably, however, a size-based difference emerged even within this group: the solo IT consulting operator (P09) focused primarily on foundational resilience principles, reflecting the resource constraints of a one-person operation, while participants from larger consulting organizations articulated more comprehensive and layered threat mitigation strategies.

Most participants agreed that while conventional threats persist, the emergence of AI has significantly increased both the scale and complexity of attacks targeting small businesses (see Fig. 8). Under traditional and persistent threats, phishing and social engineering were the most frequently cited risks, mentioned by 10 participants. As one participant noted, “Phishing and social engineering remain the number one entry point, but they have become more sophisticated with AI-generated content that makes fake emails nearly indistinguishable from real ones” (P10). The executive recruiting and staffing participant (P07, 15 employees)

offered a perspective that was notably more human-centered and less technically oriented, with threat concerns focused primarily on the human vulnerability factor rather than technical attack vectors, stating, “It's still the human element… the quality of deception is getting better, and people are more at risk than ever” (P07).

Figure 8

Modern & Evolving Threat Landscape



There was an overwhelming consensus among participants that AI represents the most significant and rapidly evolving threat landscape for small businesses, fundamentally reshaping both the scale and sophistication of cyber risks. Within the sub-theme of AI, automation, and new technologies, participants consistently identified AI as the primary emerging threat. One participant from IT consulting industry stated that AI-driven attacks, including deepfake audio and video as well as automated code generation, are becoming increasingly accessible to threat actors, significantly lowering the barrier to entry for cybercrime (P01). Another participant also from IT consulting firm emphasized the growing proliferation of AI-enabled threats, noting that attackers are leveraging AI to automate and

enhance malware, phishing, and other malicious activities, which will become increasingly problematic over the next three to five years (P06).

The healthcare IT consulting participant (P08) demonstrated threat awareness distinctly shaped by the regulatory and data sensitivity demands of the healthcare sector, with primary concerns centered on identity-based deception, AI-generated impersonation, and the internal misuse of AI tools by employees — all threats with direct implications for patient data confidentiality and HIPAA compliance. The energy sector participant (P10) demonstrated the most infrastructure-oriented threat awareness, with particular emphasis on attacks targeting critical operational systems and supply chains: “Attackers frequently exploit organizations that underestimate their risk exposure” (P10) — a warning that reflected this sector's unique exposure to threats extending beyond data confidentiality to encompass physical operational disruption.

The public sector and governance participant (P11, 200 employees) offered the most strategically sophisticated threat analysis, framing the evolving landscape not merely as a technical challenge but as a fundamental organizational transformation, and articulating the most comprehensive vision of cyber resilience as a layered integration of technical controls and organizational culture: “Resilience requires combining safeguards such as multi-factor authentication and segmentation with a blame-free culture in which employees actively contribute to security as a human firewall” (P11).

Agentic AI and autonomous systems were highlighted as particularly concerning, with participants acknowledging both their potential and the uncertainty surrounding how to effectively manage these risks (P07). In addition, the misuse of AI within organizations emerged as a critical issue. One participant explained that employees may unintentionally

expose sensitive data by integrating AI tools into their workflows, thereby creating significant security and privacy risks (P05). This concern was reinforced through real-world examples, including cases where AI systems produced inaccurate or damaging outputs that created legal and reputational consequences for organizations (P05). Deepfakes and identity-based deception were also frequently cited as growing threats. Participants noted that AI-generated impersonation—ranging from fake employees to highly convincing fraudulent communications—poses serious challenges for identity verification and fraud prevention (P08; P10).

In the category of AI-driven and emerging threats, participants highlighted how generative AI is amplifying traditional attack vectors. One participant observed, “AI-powered phishing has become a leading threat, enabling highly personalized messages and even deepfake audio that can bypass traditional training” (P11). Deepfakes, in particular, were identified as a growing concern, with one participant noting, “Deepfake video and audio now look extremely real, making it difficult to distinguish what is authentic” (P01). Another participant cautioned that the combination of AI capabilities is accelerating attack sophistication, stating that automated, AI-driven schemes can convincingly mimic legitimate requests such as financial transactions (P07).

Supply chain vulnerabilities and the rise of Ransomware-as-a-Service (RaaS) were identified as key concerns, with attackers targeting smaller organizations as entry points into larger networks (P11). Cloud misconfigurations and identity-based attacks were also noted as significant and persistent risks, particularly as businesses continue to adopt cloud technologies

(P09). Additionally, participants warned that attacks on critical infrastructure and operational technology are likely to increase as these systems become more connected (P10).

For new capabilities and strategic challenges, participants emphasized the accelerating pace of technological change as a major concern. One participant noted that while small businesses can be agile, many are unprepared for how quickly the threat landscape is evolving, requiring continuous learning and adaptation to remain secure (P03). Emerging technologies such as quantum computing were also identified as future risks, particularly in relation to the potential weakening of current encryption standards (P03; P10).

Participants emphasized that cybersecurity has fundamentally evolved from a technical concern into a core organizational strategy. One participant described this shift by noting that modern cybersecurity is no longer just an "IT problem," but a foundational business function grounded in principles such as Zero Trust— "never trust, always verify" (P11). This perspective was reinforced by another participant, who highlighted the human dimension, explaining that cybersecurity is as much about people as it is about technology, and that even the most advanced tools are ineffective without informed employees and committed leadership (P10).

Continuous education emerged as a critical component of this transformation. Participants stressed that the rapidly evolving threat landscape requires ongoing learning, with one noting that the volume of unknown and emerging risks continues to grow despite existing knowledge (P01). Another participant emphasized that attackers often stay ahead of defenders, reinforcing the need for constant awareness and education (P01). The misconception that small businesses are unlikely targets was also challenged, with

participants cautioning that this belief often increases vulnerability, as attackers frequently exploit organizations that underestimate their risk exposure (P10).

The importance of collaboration and partnerships was also highlighted. Participants noted that small businesses cannot address cybersecurity challenges in isolation and should instead rely on trusted partners and professional networks to strengthen their security posture (P03). This collective approach underscores the need for intentional and strategic action rather than reactive or minimal compliance-based efforts (P10). Participants emphasized that the goal of cybersecurity is not perfection but resilience. One participant stated that while perfect security is unattainable, consistent and risk-based practices can achieve resilient security (P09). Proactive preparedness was identified as essential, with participants advocating for always having incident response capabilities in place and ready to execute (P01).

Participants ultimately acknowledged that cyber threats are inevitable and often exceed the capacity of any single organization to manage alone (P03). As a result, the emphasis is placed on preparedness, adaptability, and strategic risk management. In conclusion, cybersecurity must extend beyond technical controls to become an integral part of business strategy. By prioritizing resilience over perfection and fostering a proactive, people-centered culture, organizations can transform cybersecurity into a strategic enabler that supports long-term sustainability in an increasingly complex threat environment. Overall, the findings indicate that AI is not only amplifying existing threats but also introducing entirely new attack vectors and strategic challenges. The convergence of AI, automation, and rapidly evolving technologies is creating a dynamic threat environment in which small businesses must continuously adapt, remain informed, and proactively address both technical and human-centered risks.

Chapter Five

Discussion

Introduction

The purpose of this qualitative study was to explore cybersecurity strategies employed by small business leaders to protect their businesses from cyberattacks in the post-COVID-19 environment. Building on the results presented in Chapter 4, this section moves beyond description to examine the meaning and significance of the identified themes. This chapter provides a summary of the findings, engages with the results, addresses limitations, explores implications for policy and practice, offers recommendations for future research, and concludes the discussion.

The findings contributed new knowledge regarding the centrality of resource constraints in shaping security capability for small businesses, challenged existing assumptions about the strategic reorientation of cybersecurity as a business imperative, and extended the literature on the transformation of the threat landscape in the age of AI, the human firewall and the imperative of psychological safety, and the measurement gap and its implications for accountability. Participants reported an increase in cyber threats, particularly phishing and ransomware, due to the shift to remote work, and contributed practical insights regarding the need for robust cybersecurity measures including employee training, contingency planning, and the use of MFA.

The single most important contribution of this study beyond existing literature is the discovery that psychological safety — not technology, budget, or technical expertise alone — is the foundational determinant of effective cybersecurity culture in small businesses. This finding introduces a human-centered, leadership-driven model of security resilience that prior

research has not systematically examined, establishing a direct empirical link between transformational leadership behaviors and cybersecurity outcomes in small businesses. Equally significant is the finding that threat perception and strategic response vary meaningfully by industry context, organizational size, and leadership maturity — dimensions that existing literature has largely overlooked in favor of generalized guidance that fails to account for the vastly different realities across the small business landscape.

The chapter concludes by acknowledging the limitations of the study, including potential biases and the geographic focus, and emphasizes the need for ongoing investment in cybersecurity infrastructure. It calls for policymakers to support small businesses in enhancing their cybersecurity measures, ensuring they can operate securely in an increasingly digital world.

Discussion of Findings

The discussion focuses on how the findings of this study contribute to the existing cybersecurity literature by illuminating the evolving role of cybersecurity as a strategic business imperative shaped by technological change, resource limitations, and an increasingly complex threat landscape. Particular attention is given to the interplay between human behavior, organizational leadership, and technical controls — areas where this study makes its most distinctive contributions beyond what prior research has established. The chapter also examines how the growing influence of AI on both defensive and adversarial capabilities is reshaping the threat environment in ways that existing small business cybersecurity frameworks have not yet adequately addressed, and how small business leaders navigate real-world trade-offs between cost, expertise, and security effectiveness in ways that challenge the generalized, one-size-fits-all guidance that currently dominates the literature.

To strengthen the theoretical contribution of the study, the findings are interpreted through established frameworks, including Transformational Leadership Theory, the National Institute of Standards and Technology Cybersecurity Framework, and Enterprise Risk Management. This alignment provides a structured lens for understanding how leadership, risk management, and cybersecurity practices converge in small business contexts.

The discussion is organized around the major themes identified in the analysis, highlighting both consistencies with prior research and new insights that emerged from participant perspectives. Collectively, these findings contribute to a deeper understanding of how small businesses can develop resilient, practical, and strategically aligned cybersecurity approaches in an increasingly dynamic and high-risk digital environment.

Alignment of Findings with Theoretical Frameworks

The findings of this study align closely with TLT, the NIST CSF, and ERM, reinforcing the study's theoretical foundation and demonstrating how leadership, structured controls, and risk-based decision-making collectively shape cybersecurity practices in small businesses.

Transformational Leadership Theory (TLT)

The findings of this study demonstrate strong alignment with TLT, particularly in the areas of leadership influence, cultural change, employee empowerment, and continuous learning. Transformational leadership emphasizes inspiring and motivating employees, fostering a shared vision, and promoting behavioral changes that were consistently reflected in participants' responses (Bass & Riggio, 2006). Participants consistently emphasized that cybersecurity is not merely a technical function but a people-centered organizational responsibility, requiring visible leadership commitment. Leaders who actively promote

cybersecurity awareness, model secure behaviors, and encourage continuous learning foster environments where employees act as proactive defenders rather than passive participants.

First, *idealized influence and leadership commitment* were evident in the way participants described the role of leaders in shaping cybersecurity as a strategic priority. Leaders who actively model security behaviors and prioritize cybersecurity create a culture where security is taken seriously across the organization. As one participant noted, *"cybersecurity is ultimately a people problem as much as it is a technology problem. You can have the best tools in the world, but if your people aren't aware and your leadership isn't bought in, you're still vulnerable."* (P10). This reflects the transformational leader's role in setting expectations and influencing organizational values.

Second, *inspirational motivation* aligns with the shift from viewing cybersecurity as a technical issue to a shared organizational mission. Participants emphasized that leaders must communicate the importance of cybersecurity in business terms and inspire employees to take ownership. For example, one participant stated, *"To really treat cybersecurity as not a technological issue, but more of a whole business strategy… everything is interconnected."* (P02). This demonstrates how leaders articulate a compelling vision that motivates collective engagement.

Third, the findings strongly support *individualized consideration and employee development*, particularly through training and awareness. Participants repeatedly highlighted the importance of continuous education and empowering employees as a "human firewall." One participant emphasized, *"The best response is the first response, which is that employee… as long as your employees are trained… that's half the battle."* (P01). This

reflects transformational leaders' focus on developing individuals' capabilities and confidence.

Fourth, *intellectual stimulation* is reflected in the emphasis on adapting to evolving threats, especially AI-driven risks. Leaders are expected to encourage critical thinking, continuous learning, and innovation in response to emerging challenges. As one participant noted, *"you have to constantly educate yourself and educate your employees… staying ahead."* (P01). This aligns with the transformational leadership principle of challenging existing assumptions and fostering proactive problem-solving.

Finally, the emphasis on *psychological safety and a blame-free culture* directly aligns with transformational leadership's focus on trust and empowerment. Participants highlighted that employees should feel safe reporting incidents without fear of punishment, reinforcing open communication and shared responsibility. This supports a culture where employees are motivated to act in the organization's best interest.

Not all participant responses, however, were fully explained by the transformational leadership framework. Several participants described adopting highly directive, top-down security mandates — strict access controls, non-negotiable password policies, and zero-tolerance enforcement measures — that reflect transactional rather than transformational leadership characteristics, suggesting that small business cybersecurity leadership in practice is more hybrid and context-dependent than any single framework can fully capture. Additionally, a small number of participants expressed skepticism about employee autonomy in security decision-making, preferring to centralize control entirely — a tension between empowerment and control that the transformational leadership framework does not fully reconcile, and that points to the need for a more nuanced theoretical model that

accommodates the pragmatic and resource-constrained leadership approaches that characterize small business cybersecurity in practice.

NIST Cybersecurity Framework (NIST CSF)

The study findings also align closely with the structure and principles of the NIST CSF, particularly its five core functions: Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2018). The NIST CSF is particularly well-suited for small businesses because it is voluntary, cost-flexible, and designed to be scalable across organizations of varying sizes, technical capabilities, and resource levels — making it accessible to businesses that lack dedicated cybersecurity staff or large IT budgets (National Institute of Standards and Technology, 2018). Participants' recommendations and practices map directly onto these domains. The findings further reflect the framework's emphasis on continuous improvement and adaptability, particularly in response to emerging threats such as AI-driven attacks (see Table 6). This demonstrates the applicability of NIST CSF as a flexible and scalable model for small businesses operating under resource constraints. Overall, the findings demonstrate that even without explicitly referencing the framework, small business leaders are implementing practices that align with the NIST CSF, reinforcing its applicability as a practical and scalable model for improving cybersecurity posture in resource-constrained environments.

Enterprise Risk Management (ERM) Framework

The results also demonstrate strong alignment with ERM principles, which position risk management as an integral part of organizational strategy (COSO, 2017). Participants consistently framed cybersecurity as a risk management issue rather than a purely technical

function, highlighting the need to prioritize resources based on potential impact and likelihood rather than relying solely on compliance requirements.

Table 6

Alignment of Findings of the Study with the NIST CSF Functions

NIST Function	Study-Aligned Practices	Description
Identify	Risk assessments; asset inventory; identification of critical business functions	Participants emphasized understanding what assets exist, what matters most ("crown jewels"), and where risks originate as the foundation of cybersecurity strategy.
Protect	MFA; strong password policies; employee training and awareness	Core preventive controls were consistently identified as essential, particularly identity-based protections and building a "human firewall" through training.
Detect	Monitoring tools; SIEM systems; phishing simulations	Early detection capabilities were supported through continuous monitoring and behavioral metrics (e.g., phishing click rates, reporting rates).
Respond	Incident response plans; defined roles and responsibilities; coordinated communication	Participants highlighted the need for structured response processes, clear decision authority, and cross-functional coordination during incidents.
Recover	Backup strategies (e.g., 3-2-1-1 rule); disaster recovery planning; business continuity plans	Emphasis was placed on resilience through tested backups, rapid restoration capabilities, and maintaining operations during and after cyber incidents.

Practices such as risk assessments, gap analyses, and prioritization of critical assets reflect ERM's structured approach to risk identification and mitigation. One participant explained, *"it was the risk assessment, and then doing gap analysis… looking at the current*

state and finding any gaps… to align with industry standards" (P02). This aligns with ERM's focus on systematically identifying and evaluating risks that could impact organizational objectives. Participants emphasized foundational controls such as MFA, employee training, monitoring systems, and secure configurations. These controls represent practical risk responses within an ERM framework, where mitigation strategies are prioritized based on risk severity and resource constraints.

The findings highlight risk response and resilience planning, including incident response, business continuity, and disaster recovery strategies. Participants stressed preparedness and the ability to maintain operations during disruptions. As one participant stated, *"the goal is to reduce the 'blast radius' of inevitable attacks… ensuring that a security incident remains a manageable operational hurdle rather than an existential catastrophe"* (P11). This aligns with ERM's focus on resilience and continuity as core components of risk management.

Finally, the study underscores strategic integration of risk management into business decision-making, a central tenet of ERM. Participants emphasized that cybersecurity must be embedded into overall business strategy. As one participant stated, *"to really treat cybersecurity as not a technological issue, but more of a whole business strategy"* (P02). This reflects ERM's holistic approach, where risk management is integrated into governance, leadership, and organizational culture.

The inclusion of cyber insurance as a financial risk transfer mechanism further supports ERM's focus on managing residual risk. One participant explained, *"cyber insurance acts as a financial backstop by transferring the high costs… away from the company's balance sheet"* (P11). This directly corresponds to ERM strategies for risk

financing and transfer. Additionally, the emphasis on leadership accountability and integration of cybersecurity into business decision-making aligns with ERM's enterprise-wide perspective on governance and risk ownership. This integration of cybersecurity into broader organizational risk strategy reinforces ERM's emphasis on holistic, organization-wide risk governance.

Overall, the findings indicate that effective cybersecurity in small businesses is achieved through the intersection of leadership, structure, and risk management. Transformational leadership drives a culture of awareness and accountability; the NIST CSF provides a structured approach to managing security activities, and ERM ensures alignment with organizational risk tolerance and strategic priorities. Together, these frameworks support a shift from reactive, compliance-based security toward a proactive, resilient, and business-integrated cybersecurity posture.

Thematic Discussion of Findings

The thematic analysis revealed a set of interconnected patterns that collectively explain how small business leaders approach cybersecurity in a rapidly evolving, post-pandemic environment. These themes provide a structured understanding of the challenges, priorities, and strategies identified by participants, moving beyond isolated observations to highlight broader organizational and behavioral dynamics.

The findings are organized into key themes that reflect both operational realities and strategic considerations, including resource constraints, the elevation of cybersecurity as a business imperative, the transformation of the threat landscape, the critical role of employees as a "human firewall," and the persistent gap in meaningful security measurement. Together, these themes illustrate that cybersecurity in small businesses is not driven by a single factor,

but rather by the interaction of leadership decisions, human behavior, technological capabilities, and external pressures.

The Centrality of Resource Constraints in Shaping Security Capability

The findings of this study demonstrate that the most serious and widespread impact on cybersecurity implementation of small businesses is the resource constraints. In all questions about the interview, the respondents always cited financial limitations, shortage of expertise, and limitations of human capital as the major determining factors on what security measures could be taken by the organizations in actual situations. This observation is consistent with the current literature that has reported the resource issues encountered by the smaller organizations in the cybersecurity sector (Kezron, 2025), but the current study builds on this by showing how such constraints flow on to the various levels of organizational security.

The interviewees expressed a core paradox that defines the small-business security environment: the more vulnerable these organizations are to attacks by advanced threat actors, the less resources they have to protect themselves; yet their vulnerability, in financial and operational terms, to successful attacks can be disproportionately high relative to other businesses. According to Kezron (2025), small businesses face insufficient financing, staff training, and formal security implementation. He suggested merging internal monitoring with external MSSPs. This tension was also concisely described by one participant in the discussion, who stated that the heightened exposure of small businesses to risks was the direct result of remote work and digital transformation, which had greatly increased the attack surface, but big businesses had historically been the primary victims. The imbalance between the sophistication of threats and the resources available to address them has created a

vulnerability gap; this gap has become a characteristic feature of the small-business security environment today.

The in-house and outsourcing controversy that appeared in the findings is the real-world reflection of the fact that most small businesses must undertake hard trade-offs between control, cost, and capability. The hybrid model of external and internal supervision was selected as the most desirable one, as it enabled firms to use expert knowledge that they could not afford to acquire within the company, but retained enough organizational knowledge to keep them on track towards the business goals. This conclusion has an important implication on the managed security service provider (MSSP) market, indicating that to ensure effective partnerships, it is necessary not only to have technical proficiency but also to be able to transform security concepts into business-relevant terminologies and integrate with the rest of the organizational system and processes. Respondents who were satisfied with the outsourcing arrangements always stressed the role of locating outside firms that were able to appreciate their business environment as opposed to providing generic security services.

The Strategic Reorientation of Cybersecurity as Business Imperative

The second significant theme that can be observed based on the data is that cybersecurity has shifted towards becoming a strategic business necessity rather than a technical IT task. The interviewees would always redefine security as a cost center, or compliance drain, but as the cornerstone of operational stability, customer confidence, and business sustainability. This transformation is especially pronounced when it comes down to the small business environment, where resources are limited, and any business investment should be paid in terms of a tangible business value.

The results show that such strategic change needs and demands an active leadership involvement that goes way beyond budget consent. Leaders who make cybersecurity a business imperative, meaning leading by example, dedicating specific resources of the organization, and bringing the issue of security into the context of strategy-making, develop organizational cultures in which security becomes the business of all people and not an IT issue. On the other hand, companies in which executives ignore controls or make security a technical feature find it difficult to attain significant security maturity, irrespective of the kind of tools they use. This finding is consistent with the current literature on the significant importance of leadership in the process of forming the security culture (Sarabi et al., 2025), but the current research shows that in small organizations with a less rigid hierarchy, the impact of leadership can be even greater and more direct.

The findings also indicate that the leadership of security in small businesses will need a specific orientation: the leaders should be capable of presenting the business case of security investments in a language that will appeal to operational and financial interests, and at the same time, they have to show their personal commitment to security practices by being able to adhere to them consistently. This twofold mandate of carrying out strategic communication and visible modeling is quite a challenge to small business leaders who might not be experts in the field of security but are required to take the lead in promoting the cause in their organizations.

The Transformation of the Threat Landscape in the Age of Artificial Intelligence

One of the most interesting conclusions, perhaps, is related to the way participants view the fundamentally altered threat landscape, which is largely fueled by the advent of generative AI. Although all the conventional cybercrimes, such as phishing and ransomware,

are still in high order, the results show a qualitative change in the magnitude, nature, and availability of attacks that most small businesses are unprepared to respond to. The AI-based threats that were consistently cited by participants as the most pressing emerging risks to their organizations are deepfakes, AI-generated phishing, and Agentic AI.

The changes that come with this transformation are far-reaching. The awareness training, which used to be done based on such blatant signs of malicious email as poor grammar, suspicious sender address, generic greetings, etc., is no longer effective as threat actors can compose hyper-personalized, grammatically flawless messages based on publicly available information. Furthermore, the appearance of the synthetic voice and video materials opens new tracks of deceit that cannot be observed through the traditional security awareness methods. The quality of deception, according to one participant, is improving, and a growing number of small businesses that depend on annual training based on compliance are more at risk.

The results also indicate that there is an alarming difference between awareness of threats and preparedness. Empirical evidence suggests a 45% lift in attack effectiveness when leveraging AI-driven impersonation techniques compared with traditional approaches; covers deepfakes, GenAI phishing and synthetic content (Arafah et al., 2025; Kashif et al., 2025). Although the participants showed advanced knowledge of the emergent threats, most of them admitted that their organizations do not have the resources and knowledge to successfully defend against the AI-based attacks. This underserved market indicates there is a failure in the market to offer small business-friendly, affordable security solutions to small businesses - a phenomenon that is both a policy issue that needs to be addressed as well as a business opportunity for creative service providers that will be able to fill in this gap.

The Human Firewall and the Imperative of Psychological Safety

The recurring theme in various interview questions is the importance of human factors in the process of both the formation and alleviation of security risk. The participants stressed several times that employees are the most frequent point of entry of attacks, as well as the most important protection, in case of proper training and support. This paradox is especially sharp in the sphere of small business, where security budgets often do not presuppose many technical restrictions, and the relations between employees and organization can be more personal and trusting.

The focus on psychological safety — establishing conditions where workers feel free to report possible incidents without fear of blame — represents a major shift from historical security strategies grounded in fear, punishment, and punitive enforcement. This observation fits the modern research on just culture in safety-related industries (Dekker, 2016), and it is possible that the concepts of psychological safety that have revolutionized aviation and healthcare could be applied to cybersecurity as well. This study extends prior research by demonstrating that psychological safety is not merely a desirable cultural attribute but a functionally critical determinant of cybersecurity effectiveness in small businesses — directly influencing whether employees report incidents early enough to contain damage or conceal them out of fear until consequences become unmanageable. This study contributes by providing empirical evidence from small business leaders that a blame-free, psychologically safe organizational culture, analogous to the just culture frameworks that transformed safety outcomes in aviation and healthcare, is both achievable and strategically essential in the small business cybersecurity context.

Small businesses can be especially well-positioned to develop such cultures, as they have a less stratified hierarchy, and leaders are in closer contact with their employees. The data, however, also shows that a significant number of organizations cannot achieve a balance between accountability and psychological safety and that the change in perspectives between punitive and supportive practices need to be deliberately led and reinforced. Companies that can effectively make this transition can discover that their staff is not only obedient to security policy adherence but also active participants in organizational protection.

The Measurement Gap and Its Implications for Accountability

The results indicate that there is a significant problem in measuring and demonstrating security effectiveness among small businesses. Although participants listed varied metrics — such as phishing simulation click rates, incident reporting rates, and training completion rates — there was broad agreement that most small businesses do not use metrics that meaningfully indicate actual risk reduction. Sarabi et al. (2025) proposed a novel cyber risk assessment method using publicly available technology signatures that fills the measurement gap for SMEs unable to collect conventional scanning data. This study extends prior research by revealing that the measurement gap is not solely a technical limitation but a leadership and accountability challenge. This study challenges prior assumptions by demonstrating that the metrics small businesses most commonly track — training completion rates and phishing click rates — may create a false sense of security progress by measuring activity rather than actual risk reduction.

Without meaningful measures, organizations cannot gauge the payoff on their security spending, or where they can improve, or display due diligence to the insurers, regulators, or clients. The trend towards behavioral measurements, measuring what employees do and not

what they should do, is an important change, but one that several small businesses do not have the knowledge or means to execute successfully. When organizations gather metrics and note participants, they do not have the analytical potential to give them meaningful interpretations or to transform knowledge into practical change.

Implications for Practice

The findings of this study carry several important implications for both theory and practice, particularly within the context of small business cybersecurity in a rapidly evolving, post-pandemic digital environment. First, the results reinforce the need to reconceptualize cybersecurity not as a purely technical function but as an organizational capability embedded within business strategy. This shift has implications for academic research, which must increasingly integrate perspectives from management, organizational behavior, and risk governance rather than treating cybersecurity as an isolated IT domain. The strong emphasis on leadership, culture, and decision-making suggests that future theoretical models should incorporate human and strategic dimensions alongside technical controls.

Second, the centrality of resource constraints highlights a structural inequality in cybersecurity readiness. Small businesses face disproportionately high risks while lacking the financial, technical, and human capital required to respond effectively. This suggests a need for more scalable, cost-effective security frameworks tailored specifically to resource-constrained environments. For policymakers and industry stakeholders, the implication is clear: without targeted support mechanisms such as subsidized services, shared security infrastructures, and simplified compliance frameworks, the vulnerability gap will persist or widen.

Third, the emergence of AI as a dominant threat vector has profound implications for both training and defense strategies. Traditional awareness programs based on recognizing obvious phishing indicators are becoming obsolete in the face of AI-generated, highly sophisticated attacks. This necessitates a transformation in training approaches toward adaptive, continuous, and behavior-focused learning models. It also implies that security solutions must evolve to incorporate AI-driven detection and response capabilities that can match the speed and scale of emerging threats.

Fourth, the findings related to the "human firewall" underscore the critical role of organizational culture, particularly the importance of psychological safety. The shift from punitive to supportive security cultures has implications for how organizations design training, reporting mechanisms, and internal policies. Encouraging open communication and non-punitive reporting can significantly enhance early threat detection and response. This aligns with broader organizational theory and suggests that cybersecurity effectiveness is closely tied to employee engagement and trust.

Fifth, the identified measurement gap reveals a critical weakness in how small businesses evaluate cybersecurity effectiveness. The reliance on superficial metrics such as training completion rates fails to capture actual behavioral change or risk reduction. This has implications for accountability, investment decisions, and regulatory compliance. There is a clear need for practical, accessible measurement frameworks that emphasize behavioral indicators, incident trends, and response capabilities rather than checkbox compliance.

In summary, the thematic analysis demonstrates that effective cybersecurity in small businesses is not achieved through isolated technical solutions but through an integrated approach that combines leadership culture, human behavior, organizational strategy, and

appropriately scaled technology. The findings make a clear contribution to the existing literature by establishing that the most consequential determinants of small business cybersecurity effectiveness are not technical but human and cultural — rooted in how leaders build psychological safety, communicate security expectations, and embed security thinking into the fabric of everyday business operations. Rather than confirming the technology-centric assumptions that have dominated prior research, this study reveals that small businesses which treat cybersecurity as a strategic leadership responsibility — rather than a delegated IT function — are better positioned to build genuine, sustainable resilience in the face of an increasingly complex, resource-constrained, and AI-driven threat environment.

Recommendations for Practice

Leaders of small business organizations should take a prioritized, risk-based approach to security that considers the limitations on resources and manages the most important vulnerabilities. Instead of trying to adopt overall security initiatives that may exceed what they have, leaders should start by having a clear idea of what they hold in high regard and what threat is most likely to occur. Basic controls, i.e., multi-factor authentication on all access points, frequently tested backups, routine patching, and fundamental staff training are the most cost-effective to invest in and should be undertaken first, before going more sophisticated.

Small business leaders should consider the hybrid model of security delivery seriously. Considering the impractical nature of in-house development of full security solutions, the leaders should nowadays consider strategic sourcing of services externally with the help of managed service providers, consultants, and technology partners. Nevertheless, internal ownership, i.e., a person who realizes the business context and security demands, is

the key to ensuring that external solutions are more oriented towards the organizational needs and culture. The best arrangements that were found to be successful in this study were those settings that had external competency and internal responsibility.

Psychological safety is one of the most important investments small business leaders can make that should be cultivated, but it is frequently ignored. It must be made clear by the leaders that reporting possible security incidents is an appreciated and safeguarded norm of behavior, even when a mistake was committed. Praising good catches, leveraging actual incidents as educational and not disciplinary events, and continually setting an example of openness concerning security issues will produce a culture in which employees become active contributors to security instead of security potential holders.

Policymakers and industry associations play an essential role in the effort to address the resource and expertise shortfall, limiting the security of small businesses. One of the basic interventions is the creation and distribution of available, free, or low-cost security advice that is specifically geared towards small businesses. This guidance must be structured in priority and not in a technical field, be rendered in ordinary language, and be structured to consider the resource limitations that characterize the small business environment.

A promising policy intervention is the promotion of shared services models. Resource pooling, such as shared threat intelligence, joint training initiatives, and coordinated incident response, enables small businesses to access capabilities that would otherwise be cost-prohibitive. These collective security services could be facilitated through municipalities, industry associations, or integrated into business licensing and membership frameworks. Regulatory and insurance systems should be designed to incentivize foundational security practices rather than impose complex compliance requirements that may be unrealistic for

small businesses. Incentive-based approaches, such as reduced insurance premiums, streamlined compliance pathways, or rewards for demonstrated security maturity, are likely to be more effective than punitive measures in encouraging sustained investment in cybersecurity.

Security practitioners and service providers must tailor their offerings to the realities of the small business environment, where time, expertise, and financial resources are limited. Solutions should be user-friendly, easy to deploy and maintain, and not dependent on dedicated security personnel. Providers who succeed in this space will recognize that they are delivering not only technical solutions but also peace of mind, trust, and long-term partnership. Accordingly, service providers should position themselves as educators and strategic collaborators, rather than solely technical implementers. Helping clients understand the business implications of cybersecurity and supporting the development of enduring security cultures enhances both organizational resilience and the strength of client relationships. This role requires not only technical expertise but also strong communication skills and business acumen.

Finally, providers should equip clients with meaningful, actionable metrics that extend beyond compliance checklists. Developing measurement frameworks that capture behavioral indicators, incident trends, and recovery readiness enables organizations to demonstrate risk reduction, improve accountability, and support continuous improvement in their cybersecurity posture.

Limitations of the Study

This study has several limitations that should be carefully considered when interpreting the findings. First, the participant pool was limited exclusively to male small

business leaders, which represents a significant demographic constraint. Despite active and deliberate efforts to recruit female participants — including direct outreach, personal encouragement, and extended response deadlines — no women ultimately completed the recruitment process, limiting the generalizability of the findings and precluding any exploration of how gender shapes cybersecurity leadership experiences and decision-making in small businesses. Future research should prioritize deliberate and targeted recruitment strategies to ensure meaningful gender representation.

Second, the study was geographically focused on small businesses within a single region — the Pacific Northwest of the United States — which may not reflect the diverse regulatory environments, industry compositions, cultural contexts, economic conditions, and cybersecurity threat landscapes experienced by small businesses in other parts of the United States or internationally. While the findings are most directly applicable to small businesses in this region, they cannot be fully generalized across all geographic contexts without additional validation through geographically diverse replication studies.

Third, the sample, although varied in terms of participant roles and organizational settings, may not be entirely representative of the broader small business population. Professional networks and industry associations were used to recruit participants, which likely produced a sample of individuals who are above average in security awareness and maturity compared to the general small business population. This raises important concerns about self-selection bias — individuals with a pre-existing interest in or commitment to cybersecurity were considerably more motivated to volunteer for participation, meaning that the small business leaders who are least engaged with cybersecurity and arguably most vulnerable are entirely absent from this study. This possible selection bias implies that the findings may

overestimate the level of cybersecurity awareness and practice typical of small businesses, and may underrepresent the significant challenges faced by organizations with little to no cybersecurity engagement, infrastructure, or leadership commitment.

Fourth, the qualitative research design, although offering rich and contextual insights that capture the complexity of participant experiences, inherently restricts the ability to generalize findings beyond the studied sample. The identified themes reflect the perspectives of a small, purposively selected group of individuals and may not be representative of all small business environments. Establishing the prevalence and generalizability of these patterns would require future quantitative research with larger and more diverse samples capable of testing the themes identified here at scale.

Fifth, the findings are based entirely on participant perceptions and self-reported practices, which are not necessarily consistent with objective security measures or verifiable organizational realities. Participants may have overstated their security competencies, underreported vulnerabilities, or described aspirational practices rather than actual behaviors — a well-documented limitation of self-report methodologies that must be carefully considered when interpreting the findings. The absence of independent verification of participants' reported security practices represents a constraint that future research incorporating observational or audit-based data collection methods could meaningfully address.

Finally, the rapidly evolving threat landscape — particularly regarding AI and its accelerating consequences for cybersecurity — means that some findings may become outdated as technologies and attack methodologies continue to advance. The emergence of new AI capabilities, novel attack vectors, and shifting adversarial strategies beyond the scope

of the current study period may diminish the currency of specific threat-related findings over time, underscoring the need for ongoing and longitudinal research that can track how small business cybersecurity leadership evolves in response to a continuously changing threat environment.

Recommendations for Future Research

This study identifies several avenues for future research that could deepen understanding of cybersecurity practices in small businesses. First, longitudinal studies are needed to examine how security practices evolve in response to emerging threats over time. Such research would provide insight into the long-term effectiveness of different cybersecurity strategies and identify which interventions produce sustained improvements as organizations mature.

Second, further research should explore the mechanisms through which leadership involvement influences cybersecurity culture in small businesses. Understanding which leadership behaviors, communication strategies, and engagement approaches are most effective would offer practical guidance for fostering stronger security cultures, particularly in resource-constrained environments.

Third, comparative studies examining different service delivery models - such as in-house, outsourced, and hybrid approaches - would help identify best practices and contextual factors that contribute to successful cybersecurity implementation. This line of research could clarify when outsourcing is most appropriate, what drives effective partnerships, and how organizations can maintain oversight and accountability when relying on external providers.

Another critical area for future research is the impact of AI on small business cybersecurity. As AI technologies become more accessible and integrated into business

operations, it is essential to understand both their defensive potential and their role in enabling more sophisticated attack vectors. Research focused on how small businesses adopt AI, secure AI-driven systems, and manage associated risks would provide timely and valuable insights for both practitioners and policymakers.

Future research should examine gender differences in cybersecurity leadership, organizational security culture, and risk perception among small business leaders. Given that the current study was limited to male participants despite active recruitment efforts, a dedicated study capturing the experiences and decision-making approaches of female small business leaders would make a valuable contribution — exploring whether gender shapes security investment priorities, incident response behaviors, and risk tolerance in ways this study was unable to capture.

Future studies should also incorporate geographic comparisons examining how location influences cybersecurity practices among small businesses. Comparing businesses in large metropolitan areas versus small or rural cities would be particularly informative, as urban businesses may have greater access to cybersecurity talent and managed service providers, while those in smaller communities face distinct resource constraints, limited local expertise, and potentially different threat environments. Regional regulatory differences and industry concentration patterns across geographic areas represent additional dimensions that future research should systematically explore.

Finally, additional research is needed to examine the relationship between cybersecurity insurance and organizational security practices. Investigating how insurance requirements influence security investments, whether coverage leads to measurable improvements in security performance, and how insurance models can be structured to

incentivize stronger security controls would contribute to more effective risk management strategies and inform policy development at both the organizational and regulatory levels.

Conclusion

This study demonstrates that cybersecurity in small businesses has undergone a fundamental transformation in the post-COVID-19 environment, evolving from a narrowly defined technical concern into a comprehensive business imperative shaped by strategy, people, and risk management. The findings collectively reveal that small businesses operate within a persistent paradox: they face increasingly sophisticated and frequent cyber threats—particularly phishing, ransomware, and AI-enabled attacks—while simultaneously lacking the financial resources, technical expertise, and organizational capacity required to defend against them effectively. This imbalance creates a structural vulnerability that defines the contemporary small business cybersecurity landscape.

A central conclusion emerging from the analysis is that resource constraints are not merely operational limitations but a foundational determinant of cybersecurity capability. These constraints influence the adoption of security controls, the ability to measure effectiveness, and the extent to which organizations can engage with external expertise. As a result, many small businesses are compelled to adopt hybrid approaches that combine limited internal oversight with outsourced services. While this model offers a pragmatic pathway to accessing specialized knowledge, its success depends heavily on alignment between external providers and the organization’s business context.

Equally significant is the clear reorientation of cybersecurity as a strategic business function. The findings emphasize that organizations achieving higher levels of security maturity are those in which leadership actively integrates cybersecurity into decision-making

processes, organizational culture, and long-term planning. In such environments, security is no longer treated as a compliance requirement or cost center but as a driver of operational continuity, customer trust, and competitive advantage. Conversely, organizations that relegate cybersecurity to a purely technical domain struggle to develop meaningful resilience, regardless of the tools they deploy.

The study also highlights the profound impact of AI on the threat landscape. AI-driven attacks—ranging from highly personalized phishing campaigns to deepfake-enabled fraud—have significantly increased both the scale and sophistication of cyber threats. This evolution renders many traditional security practices, particularly static and compliance-based training models, increasingly ineffective. The findings suggest that small businesses must transition toward continuous, adaptive, and behavior-focused security practices that reflect the dynamic nature of modern threats.

Another critical conclusion concerns the role of human factors in cybersecurity. Employees are consistently identified as both the most vulnerable entry point for attacks and the most valuable line of defense. The concept of the "human firewall" underscores the importance of not only training but also cultivating a culture of psychological safety in which employees feel empowered to report incidents without fear of blame. Organizations that foster such cultures are more likely to detect threats early and respond effectively, transforming employees from passive participants into active contributors to organizational security.

The study further identifies a significant measurement gap that limits the ability of small businesses to assess and improve their cybersecurity posture. While metrics such as phishing simulation results and training completion rates are commonly used, they often fail to capture meaningful behavioral change or actual risk reduction. This lack of robust

measurement undermines accountability, complicates investment decisions, and hinders continuous improvement. Addressing this gap requires the development of accessible, practical frameworks that align measurement with real-world security outcomes.

Across all themes, a unifying conclusion emerges: cybersecurity for small businesses is inherently multidimensional. It demands the integration of foundational technical controls, continuous employee engagement, strategic leadership, and external collaboration. No single solution is sufficient in isolation; rather, resilience is achieved through a layered, adaptive approach that prioritizes risk reduction, rapid recovery, and sustained awareness.

Ultimately, the findings reinforce that perfect security is neither realistic nor necessary. What is both achievable and essential is resilient security—the capacity to anticipate, withstand, and recover from cyber incidents while maintaining core business operations. In an environment where cyber threats are inevitable and continuously evolving, small businesses that adopt proactive, people-centered, and strategically aligned approaches to cybersecurity will be better positioned not only to survive but to thrive. Cybersecurity must be understood as a business imperative that extends beyond technology to encompass people, processes, and strategic decision-making. By embracing this broader perspective, small businesses can transform cybersecurity from a perceived burden into a source of operational strength and long-term sustainability.

References

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/j.jksuci.2022.08.003

Al-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems, 15*(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

Alghamdi, A. (2022). Cybersecurity threats to healthcare sectors during COVID-19. In *Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT)* (pp. 87–92). IEEE. https://doi.org/10.1109/ICCIT52419.2022.9711659

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access, 9*, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y., Al-Sai, Z. A., & Alhayja'a, S. A. (2020). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology, 19*(1), 100059. https://doi.org/10.1016/j.jnlest.2020.100059

Anderson, E. (2020, February 20). Ransomware the new online nightmare for business. *Times Union*. https://www.timesunion.com/business/article/Ransomware-the-new-online-nightmare-for-business-15071321.php

Arafah, M., Karadsheh, L., Aburub, F., & Alhariri, S. (2025). AI-powered social engineering and impersonation attacks. In *Emerging trends in cybersecurity* (pp. 112–132). IGI Global. https://doi.org/10.4018/979-8-3373-0832-6.ch006

Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development, 38*(2), 218–226. https://doi.org/10.1177/0266666921997512

Asiry, Y. (2024). Closing the gap: Boosting women's representation in cybersecurity leadership. *Journal of Information Security, 15*, 15–23. https://doi.org/10.4236/jis.2024.151002

Bass, B. M., & Riggio, R. E. (2006). *Transformational leadership* (2nd ed.). Lawrence Erlbaum Associates.

Benmira, S., & Agboola, M. (2021). Evolution of leadership theory. *BMJ Leader, 5*(1), 3–5. https://doi.org/10.1136/leader-2020-000296

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

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

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

Caplan, N. (2013). Cyber war: The challenge to national security. *Global Security Studies, 4*(1), 93–115.

Chagadama, J., Luamba, D., & Mwema, M. (2022). Cyberattacks: A huge concern for small business sustainability. *Global Scientific and Academic Research Journal of Economics, Business and Management, 1*, 60–75. https://www.researchgate.net/publication/366621804

Check Point Software Technologies. (2020). *Cyberattack trends: 2020 mid-year report*. https://pages.checkpoint.com/cyber-attack-2020-trends.html

Check Point Research. (2025). *Cyber security report 2025: Global threat trends and intelligence*. https://research.checkpoint.com/

Chidukwani, J., Azim, T., & El-Gayar, O. (2022). Cybersecurity in small and medium-sized enterprises (SMEs): A review. *Computers & Security, 130*, 102893. https://doi.org/10.1016/j.cose.2024.102893

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

CISA. (2023). *National Cybersecurity and Communications Integration Center (NCCIC)*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/nccic

CISA. (2021). *Cyber essentials toolkit*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cyber-essentials

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. COSO. https://www.coso.org/guidance-erm

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

Creswell, J., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Creswell, J., & Creswell, J. D. (2022). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

Day, D. V., & Thornton, A. M. A. (2018). Leadership development: The nature of leadership development. In *SAGE Publications, Inc. eBooks* (pp. 354–380). SAGE Publications. https://doi.org/10.4135/9781506395029.n14

Deloitte. (2021). *Cybersecurity in a post-pandemic world*. https://www2.deloitte.com/us/en/pages/financial-advisory/articles/financial-services-cybersecurity-global-organizations.html

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

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in)congruence between clients and vendors. *Information & Management, 54*, 452–464. https://doi.org/10.1016/j.im.2016.10.002

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2021). Software security patch management: A systematic literature review of challenges, approaches, tools, and practices. *Information and Software Technology, 144*, 106771. https://doi.org/10.1016/j.infsof.2021.106771

Eiza, M., Okeke, R., Dempsey, J., & Ta, V. (2021). Keep calm and carry on with cybersecurity @ home: A framework for securing homeworking IT environment. https://www.researchgate.net/publication/348553003

El-Hajj, M., & Mirza, Z. A. (2024). Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool. *Electronics, 13*(19), 3910. https://doi.org/10.3390/electronics13193910

Francis, J. L. (2020). *International governance of non-state actors in cyberspace: Is a single entity sufficient for dispute resolution?* [Master's thesis, Naval Postgraduate School]. Defense Technical Information Center. https://apps.dtic.mil/sti/pdfs/AD1114529.pdf

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management, 7*(1), 14–26. https://www.researchgate.net/publication/389819269

Gera, S., Nehra, S., & Jitender. (2025). The evolving cybersecurity paradigm: new threats old vulnerabilities, strategic solutions in the information Age. *International Journal of Research Publication and Reviews*, *6*(sp5), 430–451. https://doi.org/10.55248/gengpi.6.sp525.1960

Graham, L. (2021). Maximizing protection in an era of remote working. *Computer Fraud & Security, 2021*(3), 16–17. https://doi.org/10.1016/S1361-3723(21)00031-2

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy, 20*(3), 109–122. https://doi.org/10.1080/08854726.2014.925660

Hashmi, E., Yamin, M. M., & Yayilgan, S. Y. (2024). Securing tomorrow: A comprehensive survey on the synergy of artificial intelligence and information security. *AI and Ethics, 5*(3), 1911–1929. https://doi.org/10.1007/s43681-024-00529-z

Henry, C., & Foss, L. (2015). Case sensitive? A review of the literature on the use of case method in entrepreneurship research. *International Journal of Entrepreneurial Behavior & Research, 21*, 389–409. https://doi.org/10.1108/IJEBR-03-2014-0054

IBM Security. (2023). *Cost of a data breach report 2023*. IBM Security and Ponemon Institute. https://www.ibm.com/security/data-breach

Internet Crime Complaint Center. (2021). *Internet crime report 2021*. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Jimmy, F. (2024). Cyber security vulnerabilities and remediation through cloud security tools. *Journal of Artificial Intelligence General Science, 2*(1), 129–171. https://doi.org/10.60087/jaigs.v2i1.102

Kashif, M., Aasimuddin, M., Ahmed, M. A., Cheekatimalla, L. B., Ansari, E. F., & Mishra, A. (2025). AI-driven CTI for business: Emerging threats, attack strategies, and defensive measures. *International Journal of Computer Science & Information Technology, 17*(5), 90–108. https://doi.org/10.5121/ijcsit.2025.17506

Kezron, E. I. (2025). Cybersecurity framework for securing cloud and AI-driven services in small and medium-sized businesses. *Journal of Tianjin University Science and Technology, 58*(6), 526–558. https://doi.org/10.5281/zenodo.15719943

Khan, M. J., Hussain, D., & Mehmood, W. (2016). Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France. *Management Decision, 54*, 1886–1907. https://doi.org/10.1108/MD-09-2015-0400

Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID-19 pandemic. *International Journal of Information Engineering and Electronic Business, 13*(2), 1–10. https://doi.org/10.5815/ijieeb.2021.02.01

Lee, J.-M., & Hong, S. (2020). Keeping host sanity for security of the SCADA systems. *IEEE Access, 8*, 62954–62968. https://doi.org/10.1109/ACCESS.2020.2983179

Leedy, P. D., & Ormrod, J. E. (2016). *Practical research: Planning and design* (11th ed.). Pearson.

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

Locke, C. (2017). Why financial services should accelerate biometrics adoption. *Management Journal, 15*(4), 407–426. https://doi.org/10.2307/255139

Madrid, M. (2021). *Protect your small business from cybersecurity attacks*. U.S. Small Business Administration. https://www.sba.gov/blog/protect-your-small-business-cybersecurity-attacks

McIntyre, G. (2020). What is the SBA's definition of small business? Fundera. https://www.fundera.com/blog/sba-definition-of-small-business

Meng, X., Chen, Y., Suo, L., Xuan, Q., & Zhang, Z.-K. (Eds.). (2023). *Big data and social computing: 8th China national conference, BDSC 2023, Urumqi, China, July 15–17, 2023, Proceedings*. Springer. https://doi.org/10.1007/978-981-99-3925-1

Merayo, N., & Ayuso, A. (2022). Analysis of barriers, supports and gender gap in the choice of STEM studies in secondary education. *International Journal of Technology and Design Education, 33*, 1471–1498. https://doi.org/10.1007/s10798-022-09776-9

Moghaddam, Y., Kwan, S., Freund, L., & Russell, M. G. (2021). A proposed roadmap to close the gap between undergraduate education and STEM employment across industry sectors. In C. Leitner, W. Ganz, D. Satterfield, & C. Bassano (Eds.),

Advances in the human side of service engineering, 266, 363–373. Springer. https://doi.org/10.1007/978-3-030-80840-2_42

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology, 11*, Article 1755. https://doi.org/10.3389/fpsyg.2020.01755

National Institute of Standards and Technology. (2021). *Cybersecurity framework: Uses and benefits of the framework*. U.S. Department of Commerce. https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

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

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

Nugroho, Y. A., Asbari, M., Purwanto, A., Basuki, S., Sudiyono, R. N., Fikri, M. A. A., & Xavir, Y. (2020). Transformational leadership and employees' performances: The mediating role of motivation and work environment. *EduPsyCouns: Journal of*

Education, Psychology and Counseling, 2(1), 438–460. https://www.researchgate.net/publication/341792763

Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B. (2024). Overcoming remote workforce cyber threats: A comprehensive ransomware and bot net defense strategy utilizing VPN networks. *Journal of Engineering Research and Reports, 26*(8), 161–184. https://doi.org/10.9734/jerr/2024/v26i81237

Olaniyi, O. O., Asonze, C. U., Ajayi, S. A., Olabanji, S. O., & Adigwe, C. S. (2023). A regressional study on the impact of organizational security culture and transformational leadership on social engineering awareness among bank employees: The interplay of security education and behavioral change. *Asian Journal of Economics Business and Accounting, 23*(23), 128–143. https://doi.org/10.9734/ajeba/2023/v23i231176

Palanisamy, R., Norman, A. A., & Kiah, L. M. (2020). Compliance with bring your own device security policies in organizations: A systematic literature review. *Computers & Security, 98*, 101998. https://doi.org/10.1016/j.cose.2020.101998

Perwej, D., 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://doi.org/10.18535/ijsrm/v9i12.ec04

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: An exercise in interviewer self-reflexivity. *Qualitative Research, 12*(2), 165–185. https://doi.org/10.1177/1468794111422107

Pizzo, R. (2023). *The effects of COVID-19 on cybersecurity and securing a post-COVID world* [Senior honors thesis, Liberty University]. Digital Commons. https://digitalcommons.liberty.edu/honors/1297

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

Rah, A. (2023). *Device management in the security of bring your own device (BYOD) for the post-pandemic, remote workplace* (Order No. 30313944) [Doctoral dissertation, University of Fairfax]. ProQuest Dissertations and Theses Global. https://www.proquest.com/docview/2800647004

Sarabi, A., Liu, M., & Ganesan, A. (2025). Scoring the unscorables: Cyber risk assessment beyond internet scans. *arXiv*. https://doi.org/10.48550/arXiv.2506.06604

Sarginson, N. (2020). Securing your remote workforce against new phishing attacks. *Computer Fraud & Security, 2020*(9), 9–12. https://doi.org/10.1016/S1361-3723(20)30096-8

Small Business Administration. (2023). *Strengthen your cybersecurity*. https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

Small Business Administration. (2021). *Frequently asked questions about small business*. Office of Advocacy. https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/

Statista. (2021). *Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted)*. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security, 119*, 102756. https://doi.org/10.1016/j.cose.2022.102756

Štitilis, D., Pakutinskas, P., Kinis, U., & Malinauskaitė, I. (2016). Concepts and principles of cybersecurity strategies. *Journal of Security and Sustainability Issues, 6*(2), 197–210. https://doi.org/10.9770/jssi.2016.6.2(1)

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health, 9*, 20552076231177144. https://doi.org/10.1177/20552076231177144

Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing, 76*(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

Thompson, J. (2023). Factors influencing cybersecurity risk among minority-owned small businesses. *Reviews of Contemporary Business Analytics, 6*(1), 29–42. https://researchberg.com/index.php/rcba/article/view/114

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration, 39*, 100604. https://doi.org/10.1016/j.jii.2024.100604

Trumbach, C. C., Payne, D. M., & Walsh, K. (2023). Cybersecurity in business education: The how to in incorporating education into practice. *Industry and Higher Education, 37*(1), 35–45. https://doi.org/10.1177/09504222221099389

Upcity. (2022). *Small businesses cybersecurity breaches increased in 2021*. https://helpdeskcavalry.com/small-business-cybersecurity-breaches-increased-in-2021/

Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion. *Electronics, 12*(20), 4299. https://doi.org/10.3390/electronics12204299

Verizon. (2022). *DBIR: Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security*. Cengage Learning.

World Health Organization. (2020). *Naming the coronavirus disease (COVID-19) and the virus that causes it*. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

Widodo, D. S. (2022). Employee performance determination: Leadership style, individual characteristics, and work culture (a study of human resource management literature). *Dinasti International Journal of Education Management and Social Science, 3*(3), 327–339. https://doi.org/10.31933/dijemss.v3i3.1108

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2022). It won't happen to me: Surveying SME attitudes to cyber-security. *Journal of Computer Information Systems, 63*(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791

Wong, L., Lee, V., Tan, G. W., Ooi, K., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Wood, T. B. (2019). An examination of the suitability of transactional, transformational and situational leadership theories in evaluating the role of gender in determining the leadership style: A comparison and contrast of three leadership theories. *American Journal of Management Studies, 4*, 2–11.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2), 311–325. https://doi.org/10.1111/ejed.12014

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

Appendix A

Interview Protocol

Date of Interview: _____ Code Assigned: _____

The central research question for this proposed study is: what cybersecurity strategies do small business leaders implement to protect and defend their businesses from cyberattacks?

The questions for the interview are as follows:

Demographic Questions:

1. What is your age?
2. What is your gender identity?
3. What is your highest level of education, and what is your field of study?
4. What is your current job title, and how long have you been in this position?
5. How long has your organization been in operation?
6. What industry does your organization primarily operate in?
7. How many employees currently work in your organization (including yourself)?

Strategic Research Questions:

8. From your perspective, how important are cybersecurity strategies in protecting organizations from cyberattacks in today's post–COVID-19 environment? Please explain.
9. Without sharing any confidential or company-specific information, what strategies do you believe are most effective for preventing, detecting, and responding to cyberattacks for small businesses?
10. In your opinion, what are the main challenges small businesses face when implementing cybersecurity strategies, and what general steps should be taken to address those challenges? [Also, having in-house cybersecurity team vs outsourcing?]

11. From your perspective, which three cybersecurity threats pose the greatest risk to small businesses in the post–COVID-19 era, and why?
12. In what ways do written cybersecurity policies and procedures help small businesses manage risk and enhance overall security practices?
13. In your opinion, how do remote work arrangements and the use of personal devices (BYOD) impact cybersecurity for small businesses, and what strategies or best practices can be implemented to mitigate these risks?
14. What are the most effective ways to communicate and enforce cybersecurity policies within an organization?
15. What steps can organizations take to foster a culture where employees feel comfortable reporting potential security incidents without fear of blame or punishment?
16. What types of cybersecurity training or awareness initiatives do small businesses typically provide? How frequently are these offered, and are they sufficient to improve employee awareness and behavior?
17. Based on your experience, what methods or metrics do small businesses use to assess the effectiveness of cybersecurity training in improving employee awareness and behavior?
18. In what ways can senior leadership effectively model and promote strong cybersecurity practices (“cyber hygiene”) within an organization?
19. In your opinion, what business continuity and incident response strategies are most important for small businesses to effectively manage and recover from a cyberattack?
20. In what ways does cyber insurance contribute to a small business’s risk management and incident response strategy? Based on your experience, would you recommend it? Please explain.

21. Which emerging cybersecurity threats and trends do you anticipate will most significantly affect small businesses within the next three to five years?
22. What advice would you offer to other small business leaders seeking to strengthen their organization's cybersecurity posture?
23. Before we wrap up, is there anything else you'd like to add or any final thoughts you'd like to share?

    Wrap up the interview by thanking the participant.

Appendix B

Participant Invitation Email

Dear Participant,

My name is Abinet Kidane, and I am a PhD candidate at Marywood University. I am conducting a study to explore what cybersecurity strategies small business leaders implement to protect and defend their businesses from cyberattacks in the post–COVID-19 environment. I found your business contact information through the U.S. Small Business Administration's public database and would greatly appreciate your participation. As a small business owner, your perspective would be extremely valuable in helping to better understand current cybersecurity challenges and best practices. The study would involve a 45-minute interview, either in person or via Zoom—whichever option is most convenient for you.

Your participation is completely voluntary and confidential. All data will be securely stored, personal identifiers will be removed, and the information will be retained for three years before being permanently destroyed. Please review the informed consent form and indicate your consent within five business days through the Qualtrics link below.

Informed Consent Link:

https://marywood.iad1.qualtrics.com/jfe/form/SV_3QPjzJnGssj09Aa

Thank you for considering this invitation, and I would be happy to provide any additional information you may need.

This study has been approved by Marywood University's Exempt Review Committee.

Warm regards,

Abinet Kidane

PhD Candidate at Marywood University

Appendix C

Participants' Confirmation of Results

Date:

Subject: Interview Transcript Review

Dear Participant,

Thank you again for taking the time to participate in this study. I sincerely appreciate your insights and contributions. Attached to this email is the transcript from our recent interview.

I kindly ask that you review the transcript carefully to ensure that your responses have been accurately captured and that any acronyms, terminology, or context-specific details are correctly represented. This step is important to maintain the accuracy and credibility of the research.

If you would like to make any corrections, clarifications, or additions, please feel free to do so directly in the attached Word document using Track Changes or by inserting comments. You are also welcome to highlight any sections you would prefer to revise for clarity or confidentiality.

Please confirm receipt of this email and return any revisions within three (3) business days. If no changes are needed, a brief confirmation indicating that the transcript is accurate would be greatly appreciated.

Thank you once again for your valuable time and contribution to this research.

Sincerely,

Abinet Kidane

PhD Candidate

Marywood University

Appendix D

IRB Informed Consent Form

TITLE: CYBERSECURITY STRATEGIES FOR SMALL BUSINESSES IN THE POST-COVID-19 ERA: A QUALITATIVE STUDY OF RISK, THREATS, AND RESILIENCE

Principal Investigator (PI): Abinet Kidane
Principal Investigator Contact Information: agkidane@m.marywood.edu
Research Advisor: Dr. Alan Levine
Research Advisor Contact Information: levine@maryu.marywood.edu

Invitation for a Research Study

You are invited to participate in a research study about what cybersecurity strategies small business leaders implement to protect and defend their businesses from cyberattacks post the COVID-19 pandemic. You were chosen because you (a) have been operating in the Seattle metropolitan area for at least three years; (b) employ less than 500 people; (c) use technology to conduct business; and (d) participate in the business's cybersecurity decision-making process. Please read this form. Ask any questions you may have before agreeing to take part in this study.

If you decide to participate in the study, please indicate your voluntary agreement to participate by selecting a consent checkbox prior to proceeding with the study. You will be given a copy of this form to keep. Refusal to participate in this study will have no effect on any future services you may be entitled to from Marywood University. Anyone who agrees to participate in this study is free to withdraw at any time with no penalty.

Purpose – About the Study

The purpose of this study is to explore cybersecurity strategies that small business leaders implement to protect their businesses from cyberattacks in the post-COVID-19 environment.

Procedures - What You Will Do

You will participate in a semi-structured face-to-face interviews or Zoom meetings that may last for about an hour and provide company documents with cybersecurity policies and procedures.

Risks and Benefits

There will be a risk to your organization in providing data or documents about its operations. You should seek permission from your organization before participating in this study.

The benefit of participating in this study may include exploring the small business sector's cybersecurity practices, protecting small business systems from data breaches, and filling gaps in the understanding and practical nature of security practices in small businesses.

Payment or Other Rewards

Due to the nature of this research being conducted for academic purposes as part of my doctorate degree, I must kindly inform you that no payment, thank-you gifts, or reimbursements will be provided for participation. Your involvement is completely voluntary, and while there is no financial compensation, your contribution will be greatly valued and appreciated.

Confidentiality

Personal information, including name and contact information, will be confidential. Any data will be presented without personal and organizational identification information. The researcher has completed training regarding the protection of confidential information in research. No personal information will be gained from participants. Audio recordings will be kept no longer than three years after the interview's publication. The records of this study will be kept private. Information used in any written or presented report will not make it possible to identify you. Only the researcher and advisor will have access to the research records. Records will be kept in a locked file. Records will be kept for 3 years. Then they will be destroyed.

Taking Part is Voluntary

Participation is voluntary. Your decision whether or not to participate will not affect your current or future relationship with the investigator[s]. It will not affect your relationship with Marywood University. You may withdraw at any time until you submit your answers. There will be no penalty. To withdraw, contact the investigator. Your information will be deleted.

Contacts and Questions

If you have questions about this study at any time, contact the principal investigator or the advisor. His contact information appears at the top of this form.

If you have questions related to the rights of research participants or research-related injuries (where applicable), please contact the Institutional Review Board at (570) 961-4782 or irbhelp@marywood.edu.

You will be given a copy of this form for your records.

Statement of Consent

By checking the consent checkbox:

- You understand what the study involves.
- You have asked questions if you had them.
- You agree to participate in the study.

Appendix E

IRB Approval

MARYWOOD UNIVERSITY
EXEMPT REVIEW COMMITTEE
Immaculata Hall, 2300 Adams Avenue, Scranton, PA 18509

DATE:	November 24, 2025
TO:	ABINET KIDANE
FROM:	Marywood University Exempt Review Committee
STUDY TITLE:	[2177923-2] *Cybersecurity Strategies for Small Businesses in the Post-COVID-19 Era: A Qualitative Study of Risk, Threats, and Resilience*
MU ERC #:	
SUBMISSION TYPE:	Amendment/Modification
ACTION:	APPROVED
APPROVAL DATE:	November 24, 2025
CHECK IN DUE DATE:	November 24, 2026
REVIEW TYPE:	Exempt Review
EXEMPT CATEGORY:	45 CFR 46.104
(d)()()	

Dear Mr. KIDANE:

Thank you for your submission of Amendment/Modification materials to your Exemption Request for this research study. Marywood University's ERC has **APPROVED** your submission. The project meets federal exemption criteria and involves minimal risk to subjects participating in the research. All

research must be conducted in accordance with this approved submission.

Please remember that informed consent is a process beginning with a complete description of the study
and assurance of subject understanding.

We have applied the ERC's approval stamp to the following documents, which have been uploaded with this letter in IRBNet. The stamp must appear on versions shared with subjects wherever possible. If it is not feasible to use the stamped versions online (e.g. some email systems or survey platforms), please ensure that the language in the transmitted versions is identical to the stamped versions.

1. Informed Consent Form
2. Advertisement

Please also note that:

- **CLOSURE REPORTING**: Upon completion of the research, you must file a closure report form via IRBNet.
- **CHECK IN REPORTING**: While there is no expiration date for exempted studies, the ERC maintains oversight of open projects. If activities will continue beyond your approval's one-year anniversary of _11/24/26_, file a check in form by that date.
- **RECORDS RETENTION**: While there is no minimum retention period for exempted studies, you must retain records for the length of time stated in your application and informed consent form.
- **DEVIATION, UNANTICIPATED PROBLEM OR SERIOUS ADVERSE EVENT REPORTING**: If any of these events occur, you must file the appropriate form immediately via IRBNet.
- **REVISION REQUESTS**: If you decide to make procedural or document changes to your approved project, you must file a revision request form for review and approval prior to implementation, except when necessary to eliminate apparent, immediate hazards to the subjects. In hazardous situations, you must file the form immediately afterward.

Forms for the reports mentioned above may be found on the ERC's website or in IRBNet's Forms library. The library appears after you begin a follow-up package within your existing project and then click the Designer button on the left menu, followed by the blue "Need forms" link on the main screen (opens library under Step 1).

If you have any questions, please contact the Research Office at 570-348-6211, x.2418 or irbhelp@marywood.edu. Please include your study title and IRBNet number in all correspondence with this office.

Thank you and good luck with your research!

Regards,
Exempt Review Committee

Appendix F

Request for Permission to Adapt a Table

Dear Author / Publisher,

I hope this message finds you well. My name is Abinet Kidane, and I am a PhD candidate at Marywood University. I am conducting a study to explore what cybersecurity strategies small business leaders implement to protect and defend their businesses from cyberattacks post the COVID-19 pandemic. I am writing to request permission to adapt a table from your publication:

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

The material I would like to adapt includes *Table 3 - Methods commonly used by cybercriminals*. This adapted material would be included in my dissertation, which will be submitted to Marywood University and may be made publicly accessible through the university's repository. Full credit and citation will be given to the original source in accordance with your guidelines. If you require a specific attribution statement or have any conditions for use, I am happy to comply. Please let me know if there are any forms or additional information you require to process this request.

Thank you for your time and consideration. I greatly appreciate your contribution to my research and look forward to your response.

Sincerely,

Abinet Kidane

PhD Candidate at Marywood University