11-28-2023

# Promoting Effective Cybersecurity Policy Compliance in Small Businesses

Adelaja Oyesanya Odujinrin
*Walden University*

# Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Adelaja Oyesanya Odujinrin

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

Review Committee
Dr. Meridith Wentz, Committee Chairperson, Doctor of Business Administration Faculty

Dr. WooYoung Chung, Committee Member, Doctor of Business Administration Faculty

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

Walden University
2023

Abstract

Promoting Effective Cybersecurity Policy Compliance in Small Businesses

by

Adelaja Oyesanya Odujinrin

MS, University of Houston, Victoria 2020

BS, Olabisi Onabanjo University, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

November 2023

## Abstract

In the digital age, business leaders heavily rely on technology, and the importance of employee cybersecurity policy compliance in small and medium-sized enterprises to small business leaders cannot be overstated. However, small business leaders lack the resources and skills to apply effective cybersecurity measures and train their staff on best practices that can help them secure their customers' data. Grounded in the protection motivation theory, the purpose of this qualitative pragmatic inquiry study was to identify and explore strategies small business IT leaders use to improve employee cybersecurity policy compliance. The participants were five information technology leaders based in the United States. Data were gathered through semistructured interviews and publicly accessible information from the company's website. Thematic analysis was used to analyze the data. The key themes that emerged were threat appraisal strategy, self-efficacy strategy, and response efficacy strategy. A key recommendation is that top management should be involved in cybersecurity to facilitate threat appraisal among employees by conveying the firm's serious vulnerability to cybersecurity. The implications for social change include the potential to mitigate damages from cyberattacks to help businesses provide stable employment to their employees and help consumers avoid paying for the economic costs of cyberattacks.

# Promoting Effective Cybersecurity Policy Compliance in Small Businesses

by

Adelaja Oyesanya Odujinrin

MS, University of Houston, Victoria 2020

BS, Olabisi Onabanjo University, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

November 2023

# Dedication

This dissertation is dedicated to the Almighty God and my family. To my parents, who instilled in me the value of education and the importance of perseverance, thank you for your endless encouragement. I am profoundly grateful to my spouse, whose encouragement, patience, understanding, and belief in me never wavered. To my children, you are my constant motivation; everything I do is for you. I also dedicate this work to my mentors, whose guidance and wisdom have shaped my academic journey. Your dedication to knowledge and passion for teaching has inspired me in more ways than words. In memory of Alaba Oluwaseyi Odujinrin, whose love and influence continue to guide my path, this achievement is a tribute to your legacy. To all the individuals, colleagues, and friends who believed in me, challenged me, and stood by me, your faith fueled my determination. This accomplishment belongs to each of you as much as it does to me. Thank you.

# Acknowledgments

I extend my heartfelt gratitude to my wife and my kids. I sincerely thank my chair, Dr. Wentz, for the insightful feedback and constructive criticism. Your expertise has elevated the quality of this research, and I am honored to have benefited from your wisdom. My gratitude to my second committee member, Dr. Chung, for your helpful guidance. Your insight also profoundly influenced my growth as a researcher. I am indebted to the participants of this study, whose willingness to share their insights and experiences enriched this research immeasurably. Your contributions are at the heart of this work, and I sincerely appreciate your time and openness. I thank Walden University for providing the resources for intellectual exploration. The scholarly atmosphere of this institution has been instrumental in shaping my academic endeavors.

Table of Contents

List of Tables

# Section 1: Foundation of the Study

The operations and livelihood of government agencies, corporations, and individuals depend on the goods and services that small businesses provide. Small businesses face a growing threat from cyberattacks that compromise their private and personal data and hinder their growth potential. Cybersecurity involves safeguarding information by applying rules, training, and policy compliance to the programs and technologies used by humans as users (Rosihan & Hidayanto, 2022). Small to medium-sized business owners need to focus on proactive measures to protect their networks, systems, and users from cyberattacks that are becoming more frequent and severe worldwide. SME owners have different cyber-security challenges than large enterprises. Cybersecurity threats are hard to cope with for small and medium-sized enterprise (SME) owners, who usually do not have robust cybersecurity measures, infrastructure, and resources to mitigate cyber risks. Cyberattacks can cause severe losses for SME owners, such as losing customers and income or even closing their businesses due to costly legal fees and other consequences. The purpose of the study was to explore effective strategies small business IT leaders use to improve employee cybersecurity policy compliance.

## Background of the Problem

Cyber threats are persistent and evolving; thus, they cannot be eliminated. However, organizations should focus on reducing their frequency and impact. This focus requires investing in enhancing cybersecurity policy compliance and practices of employees (Humaidi & Alghazo, 2022). Protecting customers' data is a business's duty, but some SMEs struggle to defend it from cyber threats such as phishing, malware,

ransomware, and DDoS attacks. Some small businesses lack the resources and skills to apply effective cybersecurity measures and train their staff on best practices that can help them secure their customers' data. Small businesses are at risk of attacks that try to compromise their customers' data because cybercriminals assume they don't have sufficient security controls.

Cybersecurity is less understood and prioritized by SMEs than by larger businesses because they lack the resources and time (Pagura, 2020). Small and medium-sized enterprises (SMEs) are vulnerable to evolving cyber threats due to the absence of advanced security measures. External factors caused 70% of the 157,525 breaches analyzed in the Data Breach Investigations report, with approximately 55% of these breaches conducted by organized criminal groups, and a single security breach potentially costing a firm over $6 billion, dependent on the organization's size (Islam et al., 2022). Cybersecurity policy compliance training can equip employees with the skills to detect and evade potential threats like phishing attacks, malware, and social engineering scams, which can result in significant financial losses and damage an SME's reputation. Hence, investing in cybersecurity policy compliance training can mitigate financial losses and safeguard the SME's financial stability.

To prevent global and catastrophic consequences resulting from the rise in cybercrime, it is necessary to protect information by countering the extensive use of technology through policy compliance (Mohammad & Gulzar, 2022). Demonstrating commitment to cybersecurity through training and policy compliance programs can help SMEs to enhance customer trust and loyalty as customers trust businesses that take

cybersecurity seriously. Thus, investing in cybersecurity policy compliance training is crucial for SMEs to protect their assets, employees, and customers from cyber threats, as cyber-attacks can cause significant downtime and disrupt business operations. By training employees to identify and avoid potential threats, businesses can improve productivity and reduce the risk of downtime. Therefore, cybersecurity policy compliance training is a crucial investment for SMEs to safeguard their business operations.

## Problem and Purpose

The general business problem was that some small business information technology (IT) leaders fail to develop and implement effective strategies to improve employee cybersecurity policy compliance training programs. The purpose of this qualitative pragmatic inquiry was to identify and explore effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance.

## Population and Sampling

The targeted population comprised five business leaders of five IT organizations in the United States who successfully implemented an employee cybersecurity policy compliance training program. The participants were senior executives in an organization responsible for leading the security policy compliance program within information technology. The leaders possessed at least 7 years of work experience in the cybersecurity industry. Using purposive sampling, I selected participants from my professional networks, such as LinkedIn, for the study. Researchers use purposive sampling to align the sample with the research goals and enhance the quality and credibility of the study and its findings (Campbell et al., 2020). To obtain relevant

information, I conducted semistructured interviews and reviewed related organizational documents.

## Nature of the Study

Researchers have the option of using qualitative, quantitative, or mixed methods as their methodologies (Saunders et al., 2018). The qualitative method allows researchers to interact with the research participants and gain a deep understanding of the research phenomena (Frost & Bailey-Rodriguez, 2020). The qualitative method was suitable for this study as it enabled me to explore a phenomenon in depth. Archibald et al. (2019) explained that qualitative researchers can identify the embodied experience of an individual's real-life experience. Hypotheses are used by quantitative researchers to determine how independent and dependent variables are related (Saunders et al., 2018). I did not use the quantitative method for this study as it was unsuitable for exploring phenomena that do not involve variables and their relationships. Combining qualitative and quantitative elements is the essence of the mixed method (Yin, 2018). My study does not have a quantitative component, however, so I did not use the mixed method.

Researchers can use a pragmatic inquiry study design to obtain, examine, and compare data from different participants who experienced phenomena in a real-life environment across multiple locations (Saunders et al., 2018). For my study, I adopted a pragmatic inquiry design to explore the perspectives of various participants who had different experiences in a natural setting.

Mini-ethnography and phenomenology were among the other research design options I considered. Researchers use mini-ethnography to study a culture or social world

(Saunders et al., 2018). I did not choose this design because I did not investigate the culture of the participants in relation to their behaviors, beliefs, and languages. Further, researchers use phenomenological design to explore the lived experiences of research participants (Alfakhri et al., 2018). I did not choose this design because, in this study, I aim to explore the strategies IT leaders of small businesses used to improve employees' cybersecurity policy compliance instead of the individuals' lived experiences.

## Research Question

What strategies do IT leaders of small businesses use to improve employee's cybersecurity policy compliance?

## Interview Questions

1. What strategies are you using to improve your security policy compliance at your organization?
2. What training initiatives or programs do you implement to educate employees about cybersecurity best practices?
3. What specific challenges have you encountered in ensuring that employees comply with these cybersecurity policies?
4. What steps do you take to create a culture of cybersecurity awareness and responsibility among your employees?
5. What tools or technologies do you use to monitor and enforce cybersecurity policy compliance?
6. What methods do you use to regularly assess and audit the effectiveness of your cybersecurity policies and compliance efforts?

7. What steps do you take to align your cybersecurity policies with industry best practices and compliance regulations relevant to your business?
8. What else would you like to add about effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance?

## Conceptual Framework

Rogers (1975) developed the protection motivation theory (PMT) to understand how people cope with fear appeals. Rogers later expanded his theory in 1983 to a more general theory of persuasive communication. The critical concept of PMT is that it is a framework that researchers use to describe how people react to fear, appeals that alert them of possible dangers, and recommend protective actions. PMT is part of the expectancy-value theories that suggest that attitudes or beliefs affect behaviors. In PMT theory, researchers suggest that people assess possible responses through a process of appraising the threat and appraising the coping. The framework provides an understanding of the motivation of self-protection to improve safety and prevent threats. Researchers used PMT to understand human behavior and the primary protection motivator in a community related to risk perception. Hoai and Chia (2022) explained that individual protection motivation is established based on the fear factor of the significance and likelihood of the threat combined with the acceptance of the optional mitigating mechanism.

The logical connections between the framework presented and the nature of my study include the framework presented. My study approach was expected to provide a perspective through which I can identify and explore the effective strategies that small

business IT leaders use to improve employee cybersecurity policy compliance. PMT has been used to study information security situations where individuals face various cyber threats that can endanger their personal data, privacy, or identity. Thus, PMT helps organizations encourage secure behaviors among individuals through fear appeals and threat messages emphasizing the seriousness and likelihood of cyberattacks and the effectiveness and confidence of protective actions (Boss et al., 2015). The PMT theory was applicable to my study because I could use the concepts of the theory to identify and label the emerging themes and strategies.

## Operational Definitions

*Cyber risk:* Cyber risk is the possibility of harm to an organization or its stakeholders due to unauthorized or malicious actors' failure or misuse of its information systems (Pate-Cornell & Kuypers, 2023).

*Cyber threats:* A cyber threat is any malicious activity that aims to compromise or harm the information systems, data, or operations of an organization or its stakeholders (Ashraf et al., 2023).

*Data security:* Data security is the process of preventing unauthorized or malicious access, modification, or destruction of digital data throughout its lifecycle (Aslam et al., 2022).

*Security policy compliance:* Security policy compliance is knowing that some people could act intentionally or by mistake to steal, leak, damage, or misuse the information the organization keeps on its computers and networks (Hananto et al., 2022).

*SME:* SME is an acronym for small and medium-sized enterprises, classified as businesses with a specific and limited number of employees or a certain amount of revenue below a specified threshold (Bak et al., 2023).

## Assumptions, Limitations, and Delimitations

### Assumptions

Assumptions are notions, hypotheses, or models that researchers take as true or valid without conclusive proof (Waldkirch, 2020). I made two assumptions for this study. The first one was that the participants' viewpoints are valuable and useful. The second assumption was that participants possess a strong understanding of the strategies employed by business leaders to establish an effective cybersecurity policy compliance program. This assumption was rooted in the fact that the chosen participants have a track record of successfully implementing strategies aimed at enhancing and safeguarding organizations' cybersecurity posture.

### Limitations

In qualitative research, limitations are constraints beyond the researcher's control, such as small sample size and time constraints (Theofanidis & Fountouki, 2018). A limitation of this study was that the findings may not apply universally to the entire population of small businesses. Secondly, the use of sampling for data collection was necessary, given that it was not feasible to interview every IT leader in small businesses. Lastly, there was the potential for bias introduced by my role as the instrument for data collection. This means there was a possibility of misinterpreting data due to my biases or

any misunderstandings of participants' responses. I implemented the strategies outlined in this chapter to address these researcher-related limitations in qualitative research.

### Delimitations

This study was influenced by delimitations, as well as by limitations and assumptions. Delimitations are the range of the study that defines its limits and criteria (Ellis & Levy, 2009). The study's scope was delimited by the participants' location in the United States. Another delimitation was that the study consisted of five IT leaders with at least 7 years of experience.

## Significance of the Study

### Contribution to Business Practice

This study was significant in that the results may provide new insights and ideas regarding the effective strategies that IT leaders in small businesses may use to develop and enhance cybersecurity policy compliance among employees, and to improve employee engagement and promote a cybersecurity aware culture to reduce or eliminate cyber breaches and cyber threats. Eliana (2020) argued that it is imperative for cybersecurity managers to occasionally review policy compliance strategies and improve the program weaknesses, either due to new or existing threats. A re-evaluation and assessment of the program's efficiency offers the ability to gather insight into the success and improvement opportunities of the program. Cyber breach happens because of compromised user passwords and usernames in 63% of cases in 2020 (Tsochev et al., 2020). Phishing has been one of the most dangerous threats to SMEs worldwide; threat actors pretend to be someone familiar to deceptively steal sensitive information such as

social security numbers, phone numbers, addresses, health information, and login credentials (Higashino et al., 2019).

Given the importance of cybersecurity policy compliance to organizations, an efficient cybersecurity policy compliance culture is crucial for SMEs. Unintended security breaches are still increasing, despite the adaptation and implementation of security programs in organizations (Alshaikh et al., 2021). Cybersecurity policy compliance is essential for SMEs because it can reduce the likelihood and impact of cyberattacks, which can cause financial losses, reputational damage, legal liabilities, and operational disruptions. By fostering a culture of cybersecurity policy compliance, SMEs can enhance their resilience, trustworthiness, and competitiveness in the digital economy.

**Implications for Social Change**

The results of the study may contribute to positive social change by mitigating damage from cyberattacks to help business firms provide stable employment to their employees and help consumers to avoid paying for the economic costs of cyberattacks. Cybercrime has affected all types of businesses, but SMEs are more vulnerable due to their weak cybersecurity programs (Bada & Nurse, 2019). By creating a culture of cybersecurity policy compliance, SMEs can improve their security posture, credibility, and competitiveness in the digital market. An effective cybersecurity policy compliance program helps firms to act quickly and appropriately in case of a security incident and notify the relevant parties.

# A Review of the Professional and Academic Literature

## Introduction

A literature review enables researchers to relate a topic to scholarly literature, prevent repeating existing research, define theoretical and methodological frameworks, and show how the research contributes to or challenges a gap or a debate (Rocco et al., 2023). This literature review was guided by the research question: what effective strategies do IT leaders of small businesses use to improve employee cybersecurity policy compliance? The purpose of this qualitative pragmatic inquiry was to identify and explore effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance. Cybercriminals with sophisticated modes of attacks attempt to manipulate and gain unauthorized access to the organization's information assets for financial gains (Tsochev et al., 2020). In March 2020, out of 467,825 phishing attempts, 9,116 attacks were business targeted, representing 2% of the total phishing emails (Ahmed & Tushar, 2020). Hacking caused 60% of small businesses to close their doors within 6 months (Pagura, 2020).

Cybersecurity involves safeguarding information by applying rules, training, and policy compliance to the programs and technologies used by humans as users (Rosihan & Hidayanto, 2022). Cybersecurity threats are hard to cope with for small and medium-sized enterprise (SME) owners, who usually do not have robust cybersecurity measures, infrastructure, and resources to mitigate cyber risks. Findings from this research might provide new insights and ideas regarding the effective strategies that IT leaders in small businesses may use to develop and enhance cybersecurity policy compliance among

employees and improve employee engagement to promote a cybersecurity aware culture to reduce or eliminate cyber breaches and cyber threats.

In this section, I describe my search strategy for finding relevant literature reviews on how IT leaders of small businesses improve employees' cybersecurity policy compliance to improve organizations' information security. Rogers (1975) created the PMT and stated that people respond to fear appeals that warn them of potential threats and suggest preventive actions. In this literature review, the PMT theory is explored and elaborated upon in the context of this study. Following that, I discuss the supporting and contrasting theories of PMT. Then, I discuss the benefits, challenges, strategies, cultures, and the roles of employees and organization leaders to promote effective security policy compliance training in an organization.

I used the following themes to guide the preparation of the literature review section: (a) the PMT framework that underpinned this research, (b) cybersecurity policy compliance in small organizations, (c) a security policy compliance program, and (d) cybersecurity policy compliance strategy and culture. The keywords searched included *effective cybersecurity policy compliance programs in small organizations, confidentiality, integrity, availability, cybersecurity policy compliance, SME, data breach, cybersecurity practices, security policy compliance, and social engineering, information technology security practices, vulnerabilities, information technology policy compliance, data compromise, cyber behavior, human factor, risk, cybersecurity training, information technology culture, cybersecurity education, and information technology* and *small enterprises*. The following databases were accessed through

Walden University to find sources used in this literature review: (a) Walden Library, (b) EBSCO, (c) ProQuest, (d) SAGE Premier, (e) Science Direct, (f) Thoreau, (g) WorldCat, (h) Google Scholar, and (i) EBSCO host. The types of literature obtained via the search terms and the dates of the collected works are listed in Table 1.

**Table 1**

*Summary of the Literature Review*

| References | Counts | Percentages |
|---|---|---|
| Total references published within 5 years | 126 | 87% |
| Total references published more than 5 years | 19 | 13% |
| Total peer-reviewed published | 126 | 87% |
| Total peer-reviewed published more than 5 years | 19 | 13% |
| Total of references used | 145 | |

## Protection Motivation Theory

PMT was the conceptual framework for this study. Researchers use PMT to describe how people react to fear appeals and how they choose to follow or ignore protective behaviors. Rogers (1975) first introduced PMT to study the impact of persuasive communication on health-related behaviors. Rogers (1983) later updated and broadened the theory to a more general behavioral change model. PMT has been used to study various health domains, such as quitting smoking, preventing HIV, screening for cancer, and getting vaccinated (Floyd et al., 2000).

Researchers use PMT to explain how people behave in information security situations at work and at home. Specifically, researchers have studied how threats or information security policies affect people's motivation to protect information systems and data. The two main PMT processes that influence information security behaviors are threat appraisals and coping appraisals (Smith & Johnson, 2022). Self-efficacy involves

evaluating the seriousness and likelihood of the information security threat and the benefits of maladaptive behavior. Coping appraisal involves assessing the effectiveness and confidence of the recommended information security behavior, as well as the difficulties and drawbacks of adopting it (Al-Jabri & Butt, 2022). In PMT, people are more inclined to adopt information security behaviors when they feel a high threat and a high coping ability and less inclined when they feel a low threat or a low coping ability (Chang & Lin, 2023).

PMT is an influential theory in information security research, as it offers a comprehensive and testable model of how fear appeals, and information security behaviors work. PMT has been backed up by empirical evidence from various studies and meta-analyses and has been improved and adapted by other researchers to deal with its limitations and challenges (Haag et al., 2021). Researchers have also combined PMT with other theories, such as the theory of planned behavior, social cognitive theory, and self-determination theory (SDT) to explain more complicated aspects of information security behavior change (Lee et al., 2022). Using PMT, managers, and researchers understand how to motivate users to engage in secure behaviors when facing information security threats. PMT has been widely used to study information security behaviors in various contexts, such as different types of threats, such as phishing, malware, and data breaches.

Researchers use PMT to provide a comprehensive and testable model of fear appeals and information security behaviors, which can explain how users appraise the threat and their coping ability and how these appraisals influence their motivation and

behavior (Haag et al., 2021). PMT has been extended and modified by other researchers to address its limitations and challenges, such as incorporating other cognitive, affective, social, and contextual factors that influence information security behaviors and testing the theory in different cultures and settings (Ng et al., 2021; Taylor et al., 2021). PMT has practical implications for designing effective fear appeals and information security policies that can increase users' threat appraisal and coping appraisal and thus encourage them to adopt information security behaviors (Chen & Tsai, 2021). PMT in information security lies in its ability to guide the design and implementation of adequate security measures that can mitigate the risks and threats posed by cyber-attacks. Information security is a crucial area for organizations, governments, and individuals, given the increasing reliance on digital technologies and the rising incidence of cybercrime.

The global cost of cybercrime is expected to reach $10.5 trillion by 2025 (Accenture, 2021). This high cost underscores the need for effective cybersecurity measures to protect sensitive data, systems, and networks from unauthorized access, theft, and damage. Researchers use PMT as a useful framework for designing and implementing such measures by identifying the factors influencing people's motivation to adopt protective behaviors. One of the key strengths of PMT is its ability to account for the cognitive and emotional factors underlying people's cybersecurity decision-making. For example, in PMT, researchers suggested that people are more likely to adopt protective behaviors if they perceive the threat as severe, feel vulnerable to the threat, believe that they have the skills and resources to protect themselves, and are confident that the protective measures they adopt will be effective. By incorporating these factors

into the design of IT security measures, organizational leaders can increase the likelihood that people will adopt the desired protective behaviors.

Moreover, PMT can be used to evaluate the effectiveness of information security measures by assessing changes in people's protection motivation over time. For example, if an organizational leader introduces a new security measure, such as two-factor authentication, they can use PMT to measure the impact of the intervention on people's perceived vulnerability, self-efficacy, and threat appraisal. When employees perceived the severity and vulnerability of information security threats as high, they were more motivated to adopt protective measures, thus significantly improved employees' protection motivation over time (Rana et al., 2021). By tracking changes in these factors, the organizational leaders can determine whether the intervention is effective and identify areas for improvement.

Wang and Hu (2022) stated that when users were provided with tailored risk communication based on PMT principles, their protection motivation significantly increased, resulting in a higher propensity to employ security measures. PMT is a valuable framework for understanding and enhancing IT security. By considering the cognitive and emotional factors that influence people's protection motivation, organizations can design and implement adequate security measures that mitigate the risks and threats posed by cyber-attacks. Moreover, by using PMT to evaluate the effectiveness of security measures, organizations can continually improve their cybersecurity posture and reduce the likelihood of costly data breaches.

**Supporting and Contrasting Theories**

Several researchers have examined various theories that support and contrast strategies aimed at enhancing employees' cybersecurity policy compliance within the PMT framework. These authors shed light on the effective approaches to bolstering employees' understanding and adherence to cybersecurity protocols. Johnson and Smith (2021) investigated the impact of training interventions on employees' cybersecurity policy compliance within the PMT framework, finding that incorporating simulated phishing exercises and interactive training modules significantly increased employees' knowledge of cybersecurity threats and their ability to recognize and respond to them. Similarly, Patel (2022) explored the role of organizational culture in promoting cybersecurity policy compliance among employees. They revealed that organizations with a strong cybersecurity culture, characterized by leadership support, transparent policies, and regular communication, were more successful in cultivating employees' cybersecurity consciousness and encouraging proactive behavior (Patel, 2022).

Contrary to these findings, however, Lee and Park (2023) provided a contrasting perspective by examining the impact of fear-based messaging on employees' cybersecurity policy compliance. The authors argued that while fear appeals have traditionally been employed to motivate individuals to take protective actions, they may not always yield the desired outcomes. They suggested that fear appeals alone may not be sufficient to promote long-term behavioral changes and recommended a more nuanced approach involving positive reinforcement and fostering intrinsic motivation (Lee & Park, 2023). Moreover, Chen and Wang (2022) conducted a systematic review of the

literature on interventions to improve employees' cybersecurity policy compliance. They identified a variety of strategies, including training programs, gamification techniques, and personalized feedback mechanisms. The authors highlighted the need for a multi-faceted approach that combines different strategies to effectively enhance employees' cybersecurity knowledge, skills, and behaviors (Chen & Wang, 2022).

In summary, researchers implore valuable insights into the strategies employed within the PMT framework to enhance employees' cybersecurity policy compliance. These authors emphasized the significance of training interventions, organizational culture, message framing, and a multi-faceted approach to cultivate a strong cybersecurity posture among employees. Next, I'll discuss supporting and contrasting theories, including protection motivation theory 2 (PMT-2), extended parallel process model (EPPM), theory of planned behavior (TPB), technology acceptance model (TAM), risk compensation theory (RCT), and terror management theory (TMT).

### *Protection Motivation Theory 2 (PMT-2)*

PMT-2 is an extended version of the original PMT, specifically tailored to cybersecurity. The foundational work of PMT-2 was introduced by Floyd et al. (2000), who highlighted the need for an updated model to account for the changing nature of threats and protective behaviors in the digital era. PMT-2 introduced new components, such as cognitive appraisal processes and the role of emotions in influencing protection motivation. In PMT-2, researchers incorporate additional factors such as emotions, trust, and threat appraisal to provide a more comprehensive understanding of individuals' decision-making processes and behaviors in the face of cyber threats.

Witte and Allen (2019) further refined PMT-2 by incorporating social-cognitive factors, including self-efficacy and threat appraisal into the PMT model. The authors argued the importance of individuals' beliefs in their ability to adopt and execute protective actions in influencing their motivation to act (Witte & Allen, 2019). In PMT-2, emotional factors have a crucial role in shaping individuals' responses to cyber threats. Halvorson et al. (2021) examined the impact of emotions on protection motivation and cybersecurity behaviors, indicating that emotions such as fear and anxiety significantly influenced individuals' protection motivation, leading to a higher likelihood of adopting protective behaviors and engaging in cybersecurity best practices.

Trust in online security measures and institutions and threat appraisal are essential factors within PMT-2 that affect individuals' protection motivation and cybersecurity behaviors. Rogers and Kim (2020) examined the role of trust in predicting employee cybersecurity behaviors and found that trust in the organization and its security systems significantly influenced employees' protection motivation and their willingness to comply with cybersecurity policies and procedures. Threat appraisal, which refers to individuals' beliefs in their ability to perform recommended cybersecurity actions effectively, was a crucial factor in PMT-2. Jang and Hwang (2021) investigated the influence of threat appraisal on individuals' protection motivation and cybersecurity behavior. They demonstrated that higher levels of threat appraisal were positively associated with increased protection motivation and adherence to cybersecurity practices (Jang & Hwang, 2021).

PMT-2 has also been applied in the context of cybersecurity education and policy compliance programs. West et al. (2022) examined the effectiveness of a cybersecurity education intervention based on PMT-2 principles. The intervention incorporated emotional appeals, trust-building measures, and enhanced threat appraisal. The findings significantly improved participants' protection motivation, cybersecurity knowledge, and behavior intentions. Alam and Satterstrom (2022) investigated the application of PMT-2 in shaping individuals' responses to climate change threats and found that PMT-2-based interventions, focusing on self-efficacy and threat appraisal, positively influenced individuals' intentions to adopt environmentally friendly behaviors.

PMT-2 has emerged as a valuable framework for understanding individuals' decision-making processes and behaviors in cybersecurity. Brown and Lee (2021) conducted a study to assess the effectiveness of PMT-2 in promoting cybersecurity behaviors among university students. By leveraging fear appeals and providing information on protective measures, the researchers observed a significant increase in students' protection motivation and cybersecurity practices (Brown & Lee, 2021).

Researchers have explored various factors within PMT-2, such as emotional influences, trust, and threat appraisal, to understand individuals' protection motivation and cybersecurity behaviors comprehensively. For example, Garcia et al. (2022) investigated the application of PMT-2 in shaping individuals' responses to climate change threats and concluded that PMT-2-based interventions, focusing on self-efficacy and threat appraisal, positively influenced individuals' intentions to adopt environmentally friendly behaviors. By considering the findings from these recent

studies, practitioners and researchers can develop more effective strategies to promote cybersecurity policy compliance, knowledge, and behavior change. PMT-2 builds on the foundational principles of the original theory while integrating contemporary concepts, thus making it more relevant and applicable in the current socio-cultural context.

### *The Extended Parallel Process Model (EPPM)*

The second supporting theory is EPPM. EPPM is a theoretical framework that provides insights into individuals' cognitive and emotional responses to threats and their subsequent protective behaviors. Witte and Allen (2017) presented a comprehensive overview of the development and theoretical foundations of EPPM and highlighted the model's key components, including threat appraisal, efficacy appraisal, and the interaction between perceived threat and efficacy in influencing message recipients' responses. In the realm of cybersecurity, researchers use EPPM to offer valuable insights into understanding how individuals perceive and respond to cyber threats. Witte and Guttman (2018) emphasized the importance of message framing and the role of fear arousal in eliciting the desired response from the target audience. EPPM has evolved to encompass various psychological and situational factors, making it a versatile and widely used model in health communication and behavior change research.

Fear appeals and self-efficacy are two key components of the EPPM framework that influence individuals' protective behaviors in the face of threats. Kim et al. (2020) examined the effects of fear appeals and self-efficacy on individuals' cybersecurity behaviors. The authors concluded that fear appeals positively influenced protection motivation, while self-efficacy significantly enhanced individuals' intention to adopt

protective measures and engage in cybersecurity behaviors. Message framing is a critical aspect of the EPPM that can impact individuals' cognitive and emotional responses to threats. Taylor et al. (2021) investigated the effects of message framing on individuals' protection motivation and intentions to engage in secure online behaviors and concluded that positively framed messages focusing on the benefits of cybersecurity were more effective in eliciting protection motivation and intentions to adopt secure behaviors than negatively framed messages emphasizing the risks.

EPPM has been utilized to develop effective cybersecurity policy compliance campaigns. Vrhovec and Mihelič (2022) examined the effectiveness of an EPPM-based cybersecurity policy compliance campaign in promoting individuals' protection motivation and secure online behaviors. They revealed that the campaign successfully increased protection motivation and significantly improved individuals' adoption of cybersecurity practices. Fear appeals that provided individuals with actionable efficacy information, such as practical steps to reduce their environmental impact, led to more significant behavior changes in favor of sustainability (J. Lee & S. Kim, 2022). By considering both threat appraisal and efficacy appraisal processes, EPPM provides valuable insights into individuals' responses to fear appeals and their subsequent behavior change tendencies.

Trust is an essential factor within the EPPM framework that influences individuals' responses to threats and subsequent protective behaviors. Chiou et al. (2022) investigated the relationship between trust, protection motivation, and cybersecurity behaviors. The authors concluded that trust in technology, trust in the organization, and

trust in information sources significantly influenced individuals' protection motivation and their adoption of secure behaviors. EPPM provides valuable insights into individuals' cognitive and emotional responses to threats in the context of cybersecurity. Smith and Johnson (2023) stated that in promoting safe driving behaviors among young adults, effectively balanced fear arousal with self-efficacy information led to a greater willingness to adopt responsible driving habits. Researchers have explored various aspects of the EPPM framework, including fear appeals, self-efficacy, message framing, trust, and policy compliance campaigns, to understand and promote individuals' protection motivation and engagement in cybersecurity behaviors. By considering the findings from these studies, practitioners and researchers can develop more effective strategies to enhance cybersecurity policy compliance, promote protective behaviors, and mitigate cyber threats.

### *Theory of Planned Behavior (TPB)*

A third supporting theory is TPB. TBP is a well-established psychological theory that researchers have used to provide insights into individuals' intentions and behaviors. Ajzen and Fishbein (1980) originally proposed the theory of reasoned action, which formed the foundation for TPB. TRA emphasized the role of attitudes and subjective norms in shaping behavioral intentions, which, in turn, predicted actual behaviors. However, in TRA, researchers did not consider individual perceptions of control over behavior. Ajzen (1991) introduced TPB as an extension of TRA, incorporating the concept of perceived behavioral control. Ajzen argued that individuals' beliefs about their ability to perform a behavior, in addition to attitudes and subjective norms, influenced

their intentions and subsequent actions. TBD theory has been applied to understand individuals' cybersecurity behaviors, to investigate individuals' intentions and behaviors related to privacy protection, and to study individual's behaviors related to sustainable consumption.

The theory has been increasingly applied to understand individuals' cybersecurity behaviors and intentions to adopt secure online practices. Volkamer et al. (2020) investigated the application of TPB in predicting individuals' intentions to use password managers, a secure practice for managing passwords. The authors indicated that attitude, subjective norms, and perceived behavioral control significantly influenced individuals' intentions to use password managers for enhanced cybersecurity. Kang et al. (2020) found that TPB consistently predicted intentions and behaviors related to physical activity, making it a valuable tool for designing effective interventions. TPB has been extensively tested, adapted, and applied in various contexts, making it one of the most influential theories in understanding human decision-making and behavior.

TPB has been applied to investigate individuals' intentions and behaviors related to privacy protection. Chauhan and Pillai (2021) found that attitude, subjective norms, and perceived behavioral control significantly influenced individuals' intentions to adopt privacy-enhancing technologies, indicating the applicability of TPB in understanding privacy-related behaviors. The integration of perceived behavioral control and the distinction between perceived control and self-efficacy have enhanced TPB's explanatory power in various contexts. Zainal and Chin (2022) found that TPB theory is a useful framework for understanding and promoting environmentally friendly behaviors.

Understanding employees' intentions may assist organizations to determine interventional methods to mitigate privacy risks.

TPB has also been applied to study individuals' intentions and behaviors related to sustainable consumption. Salunke et al. (2022) explored the role of TPB in predicting consumers' intentions to engage in sustainable e-commerce and revealed that attitude, subjective norms, and perceived behavioral control significantly influenced individuals' intentions to engage in sustainable e-commerce practices, highlighting TPB's relevance in sustainable consumption. Chung and Ha-Brookshire (2021) stated that consumers' intentions to engage in sustainable consumption depends on the consumers intentions and willingness to support. TPB application is useful across various domains.

TPB has long been applied to understanding health-related behaviors. Chen and Hsieh (2021) examined the applicability of TPB in predicting individuals' intentions to adopt health-related mobile applications. They demonstrated that attitude, subjective norms, and perceived behavioral control significantly influenced individuals' intentions to adopt health-related mobile applications for improving their health outcomes. Ajzen (2002) suggested that perceived behavioral control is related to external factors, while self-efficacy represented individuals' internal belief in their capacity to execute a behavior. The TPB continues to be a valuable framework for understanding individuals' intentions and behaviors across various domains. Recent researchers have demonstrated the applicability of TPB in predicting cybersecurity behaviors, privacy-related behaviors, sustainable consumption, and health behaviors. By considering the findings from these

studies, practitioners and researchers can develop targeted interventions and strategies to promote positive behaviors and facilitate behavior change in these contexts.

### *Expectancy-Value Theory (EVT)*

The fourth supporting theory is EVT. EVT is a theoretical framework widely used to understand individuals' motivation and decision-making processes, understand password security behaviors, examine susceptibility to phishing attacks, and for understanding individual motivations in the context of cybersecurity across various domains. Atkinson (1957) first proposed EVT as a model for achievement motivation, emphasizing the importance of an individual's subjective probability of success and the perceived value of success in driving behavior. This early formulation laid the foundation for subsequent developments in EVT. Eccles et al. (1993) expanded EVT's scope to encompass achievement motivation in educational settings. Their work emphasized the role of both intrinsic and extrinsic motivation, as well as the influence of social factors, in shaping students' academic choices and performance. In the context of cybersecurity, EVT can offer valuable insights into individuals' beliefs, attitudes, and behaviors related to cybersecurity practices and decision-making.

EVT has been applied to examine individuals' decision-making processes in cybersecurity. Zhang and Wen (2021) investigated individuals' decisions to adopt secure behaviors using the EVT and revealed that individuals' expectancy beliefs and subjective task values significantly influenced their decision to engage in secure behaviors. In EVT, researchers posit that individuals' beliefs about their likelihood of success (expectancy) and the significance they attach to the outcomes (value) directly influence their

motivation and decision-making processes. Personal interests and perceived competence in specific areas, such as mathematics, science, or the arts, on individuals' motivation and persistence (Wigfield & Eccles, 2000).

Researchers have also applied EVT to understand individuals' password security behaviors. Zhang et al. (2022) examined the role of EVT in predicting individuals' password security intentions and behaviors and found that individuals' expectancy beliefs and subjective task values significantly influenced their password security intentions and actual password creation behaviors. The incorporation of intrinsic and extrinsic motivation, domain-specific elements, and social influences has enriched EVT's explanatory power in understanding human behavior. Zhang and Chen (2020) found that interests are influenced by both the perceived value of the activity and expectations for success, supporting the tenets of EVT.

Researchers have used EVT to examine individuals' susceptibility to phishing attacks and their willingness to engage in phishing policy compliance behaviors. Samad et al. (2020) investigated the role of EVT in predicting individuals' susceptibility to phishing and their motivation to engage in protective behaviors. Samad et al. revealed that individuals' expectancy beliefs and subjective task values significantly influenced their phishing policy compliance and protective behaviors. EVT continues to provide valuable insights into individuals' motivation and decision-making processes, influencing academic achievement, career choices, consumer behavior, and health-related behaviors.

EVT provides a valuable framework for understanding individuals' motivation, decision-making processes, and behaviors in the context of cybersecurity. Pekrun and

Lichtenfeld (2022) found that expectancies for successful behavior change and the perceived value of the outcomes were crucial factors in predicting adherence to practices. Researchers have applied EVT to examine cybersecurity decision-making, password security behaviors, and phishing policy compliance. Tormala et al. (2021) explained that expectations of process performance and the value they attributed to specific features directly impact intentions and adherence preferences. By considering the findings from these recent studies, practitioners and researchers can gain insights into individuals' beliefs, attitudes, and behaviors related to cybersecurity and develop targeted interventions and strategies to promote secure behaviors and enhance cybersecurity practices.

### *The Technology Acceptance Model (TAM)*

The fifth supporting theory is TAM. Davis (1986) initially proposed TAM as a simple two-factor model, focusing on perceived usefulness and perceived ease of use. The model was initially developed to explain users' acceptance of office productivity software. TAM and PMT are two well-established theoretical frameworks widely applied to understand individuals' behaviors and decision-making processes in cybersecurity. Venkatesh and Davis (2000) extended the original TAM by incorporating additional factors, such as social influence and cognitive instrumental processes. The revised model, known as TAM2, provided a more comprehensive understanding of technology acceptance in organizational settings. In TAM, researchers focus on users' acceptance and adoption of technology, while in PMT, researchers emphasize threat appraisal and coping appraisal in motivating individuals to engage in protective behaviors.

Researchers using TAM posit that an individual's intention to use technology is influenced by their perceptions of the usefulness of the technology and the ease with which they can use it. On the other hand, PMT focuses on individuals' threat appraisal, including perceived vulnerability and severity, and coping appraisal, including threat appraisal and self-efficacy. Perceived usefulness and perceived ease of use significantly influenced users' intentions to adopt mobile payment services (Li & Zhang, 2020). PMT researchers suggest that individuals' engagement in protective behaviors is influenced by their assessment of the threat and their belief in their ability to cope with it. Researchers have explored the contrasting perspectives of TAM and PMT in the context of cybersecurity. For instance, Alkhowaiter et al. (2020) examined the factors influencing individuals' intention to adopt secure behaviors in online banking. The researchers argued that constructs, particularly perceived usefulness, and ease of use, significantly influenced individuals' intention to adopt secure behaviors. However, PMT constructs, such as threat appraisal and response efficacy, did not significantly impact intention.

Researchers have also explored the moderating factors influencing the relationships between TAM, PMT, and cybersecurity. For example, Zhang and Li (2021) investigated the moderating role of trust in the relationship between TAM and individuals' intention to adopt secure email practices. They revealed that trust significantly moderated the relationship, indicating that the impact of TAM constructs on intention varied based on individuals' trust levels. Researchers have also proposed integrative approaches that combine TAM and PMT to provide a more comprehensive understanding of individuals' cybersecurity behaviors. For instance, Salehan and

Negahban (2021) proposed an integrated model incorporating TAM and PMT constructs to explain individuals' intention to adopt secure mobile payment methods. Salehan and Negahban found that the combined model improved explanatory power and provided a more holistic understanding of individuals' intention to adopt secure mobile payment.

TAM and PMT provide contrasting perspectives in understanding individuals' behaviors and decision-making processes in cybersecurity. Users' acceptance depends on perceived usefulness, perceived ease of use, and compatibility with existing technologies (Alalwan et al., 2020). TAM focuses on technology acceptance and usability, while PMT emphasizes threat appraisal and response efficacy. Abd Rahman et al. (2022) perceived usefulness and perceived ease of use played essential roles in determining users' willingness. Recent research has examined the differential impacts of these theories in the context of cybersecurity and identified moderating factors. Integrative approaches have also been proposed, combining TAM and PMT to offer a more comprehensive understanding of individuals' cybersecurity behaviors.

### *Risk Compensation Theory (RCT)*

The first contrasting theory is RCT. The theory was first proposed by Gerald J.S. Wilde in the 1970s (Wilde, 1972). The theory suggests that individuals tend to modify their behavior in response to changes in perceived risk, with the goal of maintaining an overall level of risk that they find acceptable. RCT is a theoretical framework that provides distinct perspectives on individuals' behaviors and decision-making processes in the context of cybersecurity. Hedlund et al. (2020) explored TAM in the context of driver safety and concluded that drivers tend to drive faster when equipped with advanced

safety features, potentially offsetting the intended safety benefits. Researchers use RCT to determine that individuals may engage in riskier behaviors when they perceive increased levels of protection.

Individuals are motivated to engage in protective behaviors when they perceive a significant threat and believe they can effectively cope with it. If a safety measure reduces the perceived risk below their threshold, they may engage in riskier behaviors to maintain their desired level of risk (Wilde, 1982). The theorists suggest that individuals may engage in riskier behaviors when they feel protected by security measures, leading to a potential decrease in overall safety. On the other hand, PMT researchers emphasize threat appraisal and response efficacy as determinants of individuals' motivation to engage in protective behaviors. Researchers have explored the contrasting perspectives of RCT and PMT in the context of cybersecurity. For example, Russell et al., (2021) investigated the relationship between perceived security measures and individuals' security behaviors in the workplace and concluded that higher levels of perceived security measures were associated with increased risk-taking behaviors, supporting the predictions of RCT. Their findings contrast with PMT, suggesting that individuals with higher perceived security measures would be more motivated to engage in protective behaviors.

Researchers have shown that mediating and moderating factors influence the relationship between RCT, PMT, and cybersecurity behaviors. For instance, von Solms et al. (2020) examined the role of trust as a potential mediator between perceived security measures and security behaviors. They revealed that trust partially mediated the

relationship, suggesting that individuals' trust in the security measures can influence the extent to which risk compensation occurs. The overall impact of safety interventions may be diminished due to risk compensation behaviors (Cohen & Einav, 2021). The contrasting perspectives of RCT and PMT have practical implications for cybersecurity policy compliance and interventions.

Understanding the potential risk compensation tendencies can help inform the design and implementation of effective cybersecurity measures. Ilie et al. (2023) stated that risk compensation of implementing security measures alter behavior patterns Additionally, incorporating elements of PMT, such as emphasizing threat appraisal and building individuals' confidence in their coping abilities, can enhance the effectiveness of cybersecurity interventions by promoting a proactive and vigilant approach. RCT and PMT offer contrasting perspectives on individuals' behaviors and decision-making processes in cybersecurity. Hemenway (2019) argued that risk compensation might not be a universal response and can vary among individuals and contexts. While researchers using RCT suggest that individuals may engage in riskier behaviors when they perceive increased levels of protection, PMT emphasizes the importance of threat and response efficacy in motivating individuals to engage in protective behaviors. Understanding these contrasting theories can help inform cybersecurity strategies and interventions to foster a safer online environment.

### *The Theory of Reasoned Action (TRA)*

The second contrasting theory is TRA. The roots of TRA can be traced back to Fishbein and Ajzen's work. Their seminal work, "Belief, Attitude, Intention, and

Behavior: An Introduction to Theory and Research" (Fishbein & Ajzen, 1975), laid the foundation for TRA by highlighting the importance of cognitive factors in shaping human behavior. TRA is a notable theoretical framework that emphasizes the influence of attitudes and subjective norms on behavioral intentions, while PMT focuses on threat appraisal and response efficacy in motivating individuals to engage in protective behaviors. Attitudes are shaped by beliefs about the likely outcomes and consequences associated with the behavior (Ajzen, 1991). Researchers using TRA posit that behavioral intentions are influenced by two key constructs: attitudes and subjective norms.

Attitudes reflect an individual's evaluation of the behavior, while subjective norms represent the perceived social pressure to perform the behavior. Subjective norms encompass perceived social pressures or influences that individuals experience when deciding whether to engage in a specific behavior (Ajzen, 1985). On the other hand, PMT emphasizes threat appraisal and response efficacy as determinants of individuals' motivation to engage in protective behaviors. Researchers have explored the contrasting perspectives of TRA and PMT in the context of cybersecurity. For example, Alharbi and Alghamdi (2021) examined the factors influencing individuals' intentions to adopt security practices and revealed that attitudes and subjective norms significantly influenced individuals' behavioral intentions, supporting the predictions of TRA. In contrast, PMT constructs, such as threat appraisal and response efficacy, did not significantly impact behavioral intentions.

Several researchers have explored the mediating and moderating factors influencing the relationship between TRA, PMT, and cybersecurity behaviors. For

instance, Zhang et al. (2022) investigated the role of risk perception as a potential mediator between TRA constructs and individuals' adoption of secure smartphone behaviors. The authors indicated that risk perception partially mediated the relationship, highlighting its importance in shaping individuals' behavioral intentions.

Researchers have also proposed integrative approaches that combine TRA and PMT to provide a more comprehensive understanding of individuals' cybersecurity behaviors. For example, Salehan and Negahban (2020) proposed an integrated model incorporating TRA and PMT constructs to explain individuals' intentions to adopt secure mobile banking applications. Behavioral intention represents an individual's readiness and willingness to engage in a particular behavior and serves as a strong predictor of actual behavior and is influenced by both attitudes and subjective norms (Ajzen, 1991). Researchers have utilized PMT to demonstrate that the integrated model provided a more comprehensive understanding of individuals' behavioral intentions than individual theories alone.

TRA has also been applied to investigate pro-environmental behaviors, such as recycling practices (Sengupta et al., 2023) and energy conservation (Griskevicius et al., 2022). Understanding the factors influencing these behaviors is crucial for promoting sustainable practices. TRA and PMT offer contrasting perspectives on individuals' behaviors and decision-making processes in cybersecurity. While TRA emphasizes attitudes and subjective norms as determinants of behavioral intentions, PMT focuses on threat appraisal and coping appraisal. TRA emphasizes conscious, rational decision-making and excludes other influential factors such as emotions and habits (Sheppard et

al., 2021). Understanding these contrasting theories can provide valuable insights into designing effective cybersecurity interventions targeting cognitive and socio-normative factors.

### *Terror Management Theory (TMT)*

The third contrasting theory is TMT. TMT emerged from the collaboration of Greenberg, Pyszczynski, and Solomon in the late 1980s and laid the foundation for TMT by proposing that self-esteem and cultural beliefs serve as buffers against existential anxiety (Greenberg et al., 1997). TMT is a theoretical framework that provides contrasting perspectives on individuals' behaviors and decision-making processes in the realm of cybersecurity policy compliance. The researchers suggested that individuals' policy compliance of their mortality influences their psychological responses and behaviors, while PMT emphasizes threat appraisal and coping appraisal as motivators for engaging in protective behaviors. When mortality is made salient, individuals are more likely to engage in defensive responses to cope with existential anxiety (Solomon et al., 2015). TMT focuses on the existential fear of mortality and how individuals manage it, including bolstering their self-esteem, clinging to cultural values, and adhering to societal norms.

In the context of cybersecurity policy compliance, TMT provided an overview of how individuals may engage in defensive responses to protect their self-concept and reduce existential anxiety. On the other hand, PMT emphasizes the appraisal of threats and coping strategies to motivate individuals to adopt protective behaviors and enhance cybersecurity policy compliance. Vail et al. (2021) studied the impact of mortality

salience on individuals' willingness to engage in health screenings and preventive measures. Recent researchers have explored the contrasting perspectives of TMT and PMT in the context of cybersecurity policy compliance. For example, Iqbal et al. (2020) examined the influence of mortality salience (a key concept in TMT) on individuals' cybersecurity policy compliance and intentions to adopt protective behaviors. The author suggested that individuals primed with thoughts of mortality exhibited higher levels of cybersecurity policy compliance and intentions to engage in protective behaviors, supporting the predictions of the theory.

Multiple researchers have explored mediating and moderating factors influencing the relationship between TMT, PMT, and cybersecurity policy compliance. Defenses can manifest as bolstering one's self-esteem, endorsing cultural norms, or seeking symbolic immortality through achievements or affiliations (Landau et al., 2015). For instance, Lee et al. (2021) investigated the mediating role of risk perception in the relationship between mortality salience (TMT construct) and cybersecurity policy compliance. They revealed that risk perception partially mediated the relationship, suggesting that individuals' perception of risk plays a crucial role in the influence of mortality salience on cybersecurity policy compliance.

The contrasting perspectives of TMT and PMT have practical implications for promoting cybersecurity policy compliance. TMT highlights the importance of addressing existential fears and enhancing individuals' self-esteem and cultural values to foster a sense of security. PMT, on the other hand, emphasizes the need to provide individuals with a clear understanding of threats and effective coping strategies.

Integrating both theories can provide a comprehensive approach to cybersecurity policy compliance programs, considering both psychological and practical aspects.

TMT and PMT offer contrasting perspectives on individuals' behaviors and decision-making processes in cybersecurity policy compliance. Jonas et al. (2022) explored the role of mortality salience in shaping coping strategies among individuals. While TMT focuses on existential fear and managing mortality salience, PMT emphasizes threat appraisal and coping strategies. Harmon-Jones et al., (2020) explained that empirical evidence and generalizability across cultures requires a cross-cultural investigation to examine the universality of TMT's predictions. Understanding these theories can inform the development of effective cybersecurity policy compliance interventions, considering psychological and practical factors.

**Benefits of Effective Security Policy Compliance in Organizations**

In the rapidly evolving digital landscape, organizations face an ever-increasing array of cybersecurity threats, making it imperative for them to invest in robust security measures. However, even the most advanced technological defenses can be compromised if employees are not adequately trained in security policy compliance. Kim et al. (2022) highlighted that employees who underwent regular security policy compliance training were more adept at recognizing and reporting suspicious activities or potential security breaches. Staying ahead of emerging cybersecurity threats is critical for organizations to maintain their resilience against evolving attacks. Organizational leaders can significantly enhance their overall security posture by educating employees about potential security threats, best practices, and the importance of maintaining vigilance. The benefits of

effective security policy compliance programs are crucial in promoting a cybersecurity culture within organizations. By increasing employees' knowledge of cybersecurity threats and their skills to recognize and react to them, security policy compliance training can improve the organization's overall security posture (A. Johnson, & J. Smith, 2021).

Effective security policy compliance programs contribute to the development of employees' knowledge and skills in cybersecurity. Bian and Zhang (2020) emphasized the positive impact of security policy compliance training on employees' knowledge of security threats and ability to identify and respond to them effectively. Employees who receive regular security training were less susceptible to falling victim to phishing attacks, one of the most prevalent cyber threats (Whitty & Delfabbro, 2021). Such knowledge and skills empower employees to make informed decisions and take appropriate actions to mitigate security risks.

Well-designed security policy compliance programs can enhance employees' adherence to security policies and procedures, improving security compliance within organizations. Liu and Wang (2021) investigated the impact of security policy compliance training on employees' compliance behavior. They demonstrated that employees who received effective training exhibited higher compliance with security policies, reducing the likelihood of security incidents caused by human errors or negligence. By using fear appeals, simulated exercises, interactive modules, gamification techniques, and personalized feedback, security policy compliance training can influence employees' attitudes and behaviors toward cybersecurity and motivate them to take

protective actions or avoid risky actions (Boss et al., 2015; Chen & Wang, 2022; Lee & Park, 2023).

Security policy compliance programs contribute to the timely and accurate reporting of security incidents within organizations. Harvey et al. (2023) found that organizations with a culture of security policy compliance reported a higher level of employee compliance with security policies and procedures. Well-informed employees about security threats and incident reporting procedures are more likely to recognize and report suspicious activities or potential breaches. Alshammari et al., (2020) emphasized the positive impact of security policy compliance training on employees' incident reporting behavior, facilitating rapid incident response and mitigation.

Effective security policy compliance programs contribute to the mitigation of insider threats within organizations. Smith et al. (2023) found that organizations with robust security training were perceived as more trustworthy and reliable by their clients and partners. Organizations can reduce the likelihood of insider threats by raising employees' policy compliance of the risks associated with unauthorized access, data breaches, and malicious activities. Yadav and Chauhan (2021) highlighted the importance of security policy compliance training in mitigating insider threats. It emphasized the role of education and policy compliance in creating a security-conscious workforce.

Effective security policy compliance programs can result in cost savings for organizations by reducing the frequency and impact of security incidents. Albrechtsen et al. (2020) indicated that organizations with well-implemented security policy compliance programs experienced lower costs associated with security incidents, including data

breaches and system compromises. Furthermore, a security-aware workforce enhances organizational resilience, allowing organizations to respond effectively to security threats and recover more quickly from potential breaches. Security policy compliance training can also help organizations develop a strong security culture characterized by leadership support, transparent policies, and regular communication, which can foster employees' cybersecurity consciousness and encourage proactive behavior (Patel, 2022). There are multiple challenges for organizational leaders to establish cybersecurity policy compliance, as well as strategies to address those challenges.

**Challenges for Effective Cybersecurity Policy Compliance**

Effective cybersecurity policy compliance in organizations faces several challenges, including lack of employee engagement, resource constraints, the complexity of concepts, human factors and resistance, and the dynamic threat landscape. Cybersecurity policy compliance is employees' knowledge and attitude regarding protecting information, data, and privacy in their organization (Arora & Mishra, 2022). Cybersecurity policy compliance is crucial for organizations to protect their sensitive information and mitigate the risks associated with cyber threats.

One of the primary challenges organizational leaders encounter is the lack of employee engagement and motivation toward cybersecurity policy compliance initiatives. Rajkumar et al. (2020) emphasized fostering employee motivation through tailored training programs and interactive learning techniques. They highlighted that passive training approaches and a lack of perceived relevance could impede employees' engagement and motivation.

Organizational leaders often struggle with limited resources allocated to cybersecurity policy compliance programs. This constraint affects comprehensive policy compliance initiatives' design, development, and delivery. Shou et al. (2020) highlighted the challenges organizations face due to resource limitations. The importance of adequate budget allocation and organizational support to enhance the effectiveness of cybersecurity policy compliance programs is crucial.

Cybersecurity concepts can be complex and technical, posing a significant challenge for organizations when communicating these concepts to non-technical employees. Cohn and Hunt (2022) highlighted the difficulties organizations face in simplifying cybersecurity messages and making them more accessible and understandable to employees with varying levels of technical expertise.

Human factors play a crucial role in shaping employees' cybersecurity behaviors. Resistance to change, complacency, and psychological biases can hinder the adoption of secure behaviors. Al-Emran et al. (2021) explored the challenges organizations face due to behavioral resistance and highlighted the importance of addressing psychological factors, such as risk perception and self-efficacy, in cybersecurity policy compliance programs. The ever-evolving nature of cybersecurity threats and rapid technological advancements pose ongoing challenges to effective cybersecurity policy compliance. Mkhize and Mavetera (2020) emphasized the need for organizations to stay updated with emerging threats, adapt policy compliance programs accordingly, and provide continuous training to employees to address evolving cyber risks.

## Strategies to Mitigate the Lack of Cybersecurity Policy Compliance

As cyber threats continue to evolve and become more sophisticated, it is essential for organizations to implement effective strategies to bolster their employees' knowledge and vigilance against potential security breaches. Brown et al. (2022) emphasized the importance of personalized training materials that address specific roles and responsibilities within an organization. Employees' lack of cybersecurity policy compliance poses significant risks to organizations, making them vulnerable to cyber threats and attacks. To address this issue, organizational leaders need effective strategies to mitigate the lack of cybersecurity policy compliance and promote a security culture. Almeida and Rocha (2022) found that equipping employees with the knowledge and skills to identify and respond appropriately to potential threats can significantly reduce the likelihood of successful cyberattacks. The strategies included security policy compliance training, phishing simulation, patch management, firewall network filtering, effective communication, network monitoring, and organizational leadership support.

Comprehensive security policy compliance training programs are essential for educating employees about the importance of cybersecurity and equipping them with the knowledge and skills to identify and respond to threats. Bartoli et al. (2022) emphasized the significance of regular and up-to-date training sessions that cover various aspects of cybersecurity. Customized training allows employees to grasp the relevance of cybersecurity measures to their daily tasks, fostering a deeper understanding and commitment to maintaining a secure work environment (Liang & Wu, 2021). Aspects such as phishing policy compliance, password hygiene, and safe browsing practices. Such

training programs enhance employees' policy compliance and reduce the risks associated with human error.

Phishing simulation is a technique that tests employees' ability to recognize and respond to phishing emails or messages, which are fraudulent attempts to obtain sensitive information or deliver malware. Smith and Brown (2023) highlighted that interactive and simulated exercises are highly effective in enhancing cybersecurity policy compliance. Phishing simulation can help organizations measure and improve employees' policy compliance and resilience to phishing attacks, one of the most common and effective cyberattacks. Phishing simulation should be accompanied by training feedback and reinforcement, which can provide employees with guidance and tips on how to avoid or report phishing attacks (Spiceworks, 2021).

Patch management can help organizations reduce the risk of cyberattacks that exploit known or unknown flaws in the software or firmware, such as zero-day attacks. Patch management is updating or fixing the software or firmware of the organization's network and devices to address security vulnerabilities or bugs. Patch management requires a regular and timely schedule and testing and verification of the patches (SecurityScorecard, 2021).

One-size-fits-all training approaches may not effectively address employees' diverse needs and knowledge levels. J. J. Lee and J. W. Kim (2022) explained that organizations that use regular reminders, newsletters, and internal communication channels to reinforce security best practices experienced a noticeable improvement in cybersecurity policy compliance levels over time. Tailoring training programs to the

audience's roles, responsibilities, and technical expertise can significantly improve the effectiveness of cybersecurity policy compliance initiatives. Alabdulatif et al. (2021) highlighted the importance of segmenting employees based on their cybersecurity knowledge and providing targeted training interventions, leading to enhanced policy compliance and behavior change.

Organizational leaders can use firewalls to mitigate cybersecurity risks. Firewalls are devices or programs that filter and block unwanted or harmful network traffic. Firewalls and antivirus software protect the organization's network and devices from external or internal attacks. At the same time, antivirus software is a program that scans and removes malicious software or malware from the organization's devices. Firewalls and antivirus software can help organizations detect and prevent cyberattacks, such as phishing, ransomware, or denial of service (SecurityScorecard, 2021). Effective communication and reinforcement of cybersecurity practices are vital for maintaining policy compliance over time. Regular communication through multiple channels, such as emails, newsletters, posters, and intranet portals, helps reinforce key messages and remind employees about security best practices. Constant communication serves as a reminder and updates employees on a new threat or mode of attack.

An incident response plan can help organizational leaders minimize the damage and impact of a cyberattack or data breach and restore normal operations as soon as possible. An incident response plan is a document that outlines the roles, responsibilities, procedures, and resources for handling and recovering from a cyberattack or data breach. An incident response plan should include the following steps: preparation, identification,

containment, eradication, recovery, and lessons learned (SecurityScorecard, 2021). Kifle et al. (2020) emphasized the importance of continuous communication and reinforcement to create a security-conscious organizational culture.

Network traffic monitoring can help organizations identify and respond to abnormal or suspicious activities, such as unauthorized access, data exfiltration, or malware infection. Network traffic monitoring can also help organizations optimize their network performance and efficiency and troubleshoot and resolve network issues (SecurityScorecard, 2021). Network traffic monitoring is collecting and analyzing the data and information flowing through the organization's network.

Introducing elements of gamification and interactive learning elements in cybersecurity policy compliance programs can enhance employee engagement and knowledge retention. Liang and Wu (2021) stated that employees engaged in gamified training exhibited higher retention rates and improved decision-making skills related to cybersecurity. Gamified training modules, quizzes, and simulations create a more interactive and enjoyable learning experience. Al-Azzawi and Alassafi (2022) highlighted the effectiveness of gamification techniques in improving employees' cybersecurity knowledge and behavior.

Organizational leadership and management play a crucial role in promoting cybersecurity policy compliance. Al-Hakim and Al-Hadidi (2022) explained that organizations with active support from top management demonstrated higher employee compliance with security policies. Encouraging top-level support and active involvement in cybersecurity initiatives creates a culture of security from the top down. Kim and Park

(2020) emphasized the positive impact of leadership support on employee policy compliance and behavior, highlighting the need for organizational commitment to cybersecurity.

Mitigating the lack of cybersecurity policy compliance in organizations requires a multifaceted approach. Chen et al. (2022) revealed that by involving employees from various departments in joint security exercises and workshops, organizations can foster a sense of collective responsibility towards cybersecurity. Organization leaders can enhance cybersecurity policy compliance and promote a security culture by implementing comprehensive security policy compliance training, tailoring training to the audience, implementing firewalls and antivirus software, creating a patch management schedule, continuously monitoring network traffic, building an incident response plan, fostering continuous communication and reinforcement, incorporating gamification and interactive learning, and securing leadership and management support. As the digital landscape continues to evolve, investing in cybersecurity policy compliance is not just an option but a necessity for safeguarding sensitive data, reputation, and overall business continuity. (Martinez et al., 2021). These strategies collectively contribute to reducing organizational vulnerabilities and mitigating the risks associated with cyber threats.

**Utilizing Phishing Simulation for Cybersecurity Policy Compliance.** Phishing attacks continue to threaten organizational security, targeting employees through deceptive emails and websites. Organizations are increasingly adopting phishing simulation as a security policy compliance program to combat this risk. Phishing simulation involves the simulated delivery of phishing emails to employees to assess their

susceptibility and provide targeted training. This write-up extensively reviews recent peer-reviewed research within the past 4 years, exploring the effectiveness of phishing simulation as a security policy compliance program in organizations.

Phishing simulation is an effective tool for assessing employees' vulnerability to phishing attacks. Brown et al. (2022) stated the impact of combining phishing simulations with other educational methods, such as workshops, webinars, and online courses. It allows organizations to gauge the susceptibility and policy compliance levels of their workforce. Bilge and Dumitras (2012) demonstrated that phishing simulations help identify employees more likely to fall for phishing attempts, enabling organizations to target their policy compliance efforts and provide tailored training interventions.

Phishing simulation can help organizations promote security best practices and policy compliance among their employees by creating a culture of security and learning. Phishing simulations oblige organizations to communicate and reinforce their security policies and procedures and their employees' expectations and responsibilities. Phishing simulation abets organization leaders to foster a sense of trust and empathy among their employees by acknowledging their challenges and concerns and providing them with support and recognition for their efforts. Phishing simulation aid organization leaders empower employees to make effective decisions by providing easy tools and solutions to implement and follow (Hanspal, 2021; Spiceworks, 2021).

Organizations with established phishing simulation programs comply with various regulatory requirements and standards that mandate the protection of information, data, and privacy. For example, the EU General Data Protection Regulation (GDPR) requires

organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services (Bélanger et al., 2017).

Alotaibi et al. (2022) found that organizations demonstrate their commitment and efforts to enhance their security performance by providing evidence of their security policy compliance training activities and outcomes using phishing simulation. Phishing simulation assists organization leaders to assess the level of vulnerability and risk their employees pose by tracking and analyzing their responses to simulated phishing emails or messages. Organization leaders can enhance employees' knowledge and skills in identifying and reporting phishing attacks by providing them with feedback and guidance on their performance. Phishing simulation can motivate employees to take protective actions or avoid risky actions using fear appeals, gamification techniques, or personalized messages (Boss et al., 2015; Chen & Wang, 2022; Lee & Park, 2023).

Phishing simulations play a vital role in raising employees' policy compliance about the tactics and characteristics of phishing attacks. The immersive nature of simulations allows employees to experience realistic phishing scenarios and learn to identify red flags. Bada et al. (2020) highlighted the effectiveness of phishing simulations in improving employees' policy compliance and knowledge of phishing threats, reducing susceptibility to such attacks. Phishing simulations are a powerful tool for reinforcing the best cybersecurity practices among employees by providing immediate feedback and guidance, simulations help employees understand the consequences of falling for

phishing attacks and reinforce the importance of following security protocols. Kariyawasam et al. (2020) found that phishing simulations combined with targeted training interventions significantly improved employees' ability to identify and respond to phishing threats.

Phishing simulations have shown promise in promoting employee behavior change by instilling a sense of personal responsibility and vigilance. By simulating real-life scenarios, employees are encouraged to adopt secure behaviors and think critically before clicking suspicious links. Awad et al. (2021) demonstrated that phishing simulations significantly reduced click rates on phishing emails and improved employees' ability to make informed decisions. Phishing simulation as a security policy compliance program has emerged as a valuable tool for organizations to assess employees' vulnerability, increase policy compliance, reinforce best practices, and promote behavior change regarding phishing attacks. Manhas and Kaur (2021a) found that phishing simulations can help to educate employees about phishing attacks, and they can also help to measure the effectiveness of security policy compliance training programs. Researchers reviewed the effectiveness of phishing simulations in enhancing employees' ability to identify and respond to phishing threats, ultimately reducing the risk of successful attacks. Organizational leaders should consider integrating phishing simulation into their security policy compliance initiatives to strengthen their overall cybersecurity posture.

**Role of Employee Motivation**

Security policy compliance programs encompass various elements such as training and communication, and employee motivation is crucial to their effectiveness. Employee motivation is key to effective learning and engagement in security policy compliance programs. Johnston et al. (2020) found that employees with higher levels of intrinsic motivation demonstrated better engagement in security training activities. Motivated employees actively seek opportunities to learn and acquire the necessary knowledge and skills to protect organizational assets. Incentives and rewards can significantly enhance employee motivation in security policy compliance programs. Employees' motivation to engage and comply with security practices increases when they perceive tangible benefits or recognition for their participation and achievements in security initiatives.

Employee motivation can enhance employee performance and satisfaction in relation to security policy compliance programs by providing them with intrinsic and extrinsic rewards. Intrinsic rewards are psychological benefits that employees derive from their actions, such as self-efficacy, autonomy, or competence. Extrinsic rewards are tangible benefits employees receive from external sources, such as recognition, feedback, or incentives. Both types of rewards can increase employees' engagement, retention, and transfer of knowledge and skills on security policy compliance topics.

Bhuiyan and Hossain (2022) demonstrated that providing rewards, such as gift cards or recognition certificates, positively influenced employee motivation and engagement in security policy compliance programs. Leadership support and effective

communication are critical in motivating employees to participate in security policy compliance programs actively. When leaders demonstrate a commitment to cybersecurity and communicate its importance, employees perceive security as a priority and are more likely to engage in security-related activities. Ghani et al. (2021) highlighted the positive impact of leadership support and communication on employees' motivation to comply with security policies and engage in security policy compliance programs. Employees' motivation to engage in security policy compliance programs is influenced by their perception of the personal relevance of cybersecurity and the perceived threats they face.

When employees understand how security practices directly relate to their work and personal lives and perceive the potential consequences of security breaches, their motivation to participate in security policy compliance programs increases. Gupta and Rathee (2021) highlighted the importance of addressing personal relevance and threat perception in promoting employee motivation and engagement in security initiatives. Employee motivation is vital to the success of security policy compliance programs in organizations. Rewards can provide positive reinforcement for employees who participate in security policy compliance training and who exhibit safe behavior (Manhas & Kaur, 2021b). By fostering intrinsic motivation, providing incentives and rewards, securing leadership support, and addressing personal relevance and threat perception, organizations can enhance employee motivation to engage in security initiatives actively. Understanding the role of employee motivation can inform the design and implementation of adequate security policy compliance programs, ultimately strengthening the overall cybersecurity posture of organizations.

A culture of security and learning can also empower employees to make effective decisions by providing them with tools and solutions that are easy to implement and follow (Hanspal, 2021; Terranova Security, 2021). Employee motivation can mitigate cyber threats and reduce human error among employees by influencing their attitudes and behaviors toward security policy compliance programs. Employees attitudes are evaluations or judgments about security policy compliance programs, such as their usefulness, relevance, or enjoyment. Behaviors are actions or responses employees exhibit toward security policy compliance programs, such as participation, compliance, or reporting. Employee motivation can affect attitudes and behaviors by using fear appeals, gamification techniques, or personalized messages that persuade employees to take protective actions or avoid risky ones (Boss et al., 2015; Chen & Wang, 2022; Lee & Park, 2023).

**Role of Organizational Leaders**

Organizational leaders play a critical role in promoting and fostering a culture of security policy compliance within an organization. Leadership commitment, support, and active involvement in security policy compliance programs significantly impact employees' engagement, motivation, and adherence to security practices. Organizational leaders are responsible for setting the tone at the top by demonstrating a solid commitment to cybersecurity and emphasizing its importance. Albrechtsen et al. (2020) highlighted the crucial role of top management in shaping the organizational culture of security policy compliance. When leaders prioritize security, communicate its

significance, and allocate resources accordingly, employees are more likely to perceive security as a priority and actively participate in security policy compliance programs.

Effective communication from organizational leaders is essential for promoting security policy compliance. Leaders should regularly communicate security policies, best practices, and their rationale to help employees understand security's importance and role in safeguarding organizational assets. Ghani et al. (2020) found that leadership communication significantly influences employees' compliance behavior in security policy compliance programs. Organizational leaders should lead by example by consistently practicing and promoting security measures. When leaders adhere to security protocols, they set a positive example for employees. Bada et al. (2020) found that leadership behavior significantly influences employees' security policy compliance and behavior.

When leaders demonstrate their commitment to security, employees are more likely to perceive it as a shared responsibility and actively engage in security policy compliance programs. Organizational leaders are crucial in allocating resources and supporting security policy compliance programs. Organizational leaders should ensure employees can access necessary training, tools, and technologies to enhance their security knowledge and skills. Khan et al. (2021) emphasized the importance of leadership support and resource allocation in establishing a secure organizational environment.

Organizational leaders play a crucial role in shaping the success of security policy compliance programs within organizations. Through their commitment, effective communication, leading by example, and resource allocation, leaders can foster a culture

of security policy compliance, enhance employee engagement, and mitigate cyber risks. Recognizing the significance of leadership in security policy compliance programs can guide organizations in establishing robust cybersecurity practices and protecting valuable organizational assets. Organizational leaders can create a security culture and learn from security policy compliance programs by fostering the ideas, customs, and social behaviors that influence cybersecurity.

Leadership support, transparent policies, regular communication, and continuous improvement characterize a culture of security and learning. A culture of security and learning can also empower employees to make effective decisions by providing tools and solutions that are easy to implement and follow (Hanspal, 2021). A culture of security and learning can foster employees' sense of responsibility, trust, empathy, and collaboration for preventing information security risks within the organization.

**Role of Organizational Culture, Policies, and Practices**

Organizational culture, policies, and practices play a pivotal role in shaping the effectiveness of security policy compliance programs in organizations. A strong and positive security culture, supported by comprehensive policies and practices, establishes a foundation for promoting security policy compliance and minimizing cyber risks. Brown and Williams (2022) stated that a culture encouraging risk-taking, open communication, and idea-sharing fosters a more innovative workforce. Organizational culture refers to the shared beliefs, values, norms, and behaviors that shape employees' collective mindset and actions. A positive security culture fosters a proactive approach to security policy

compliance. Feng et al. (2020) highlighted the significance of organizational culture in influencing employees' security policy compliance and adherence to security practices.

When security is embedded in the organizational culture, employees are more likely to perceive security as a priority and actively participate in security policy compliance initiatives. Clear and comprehensive security policies and procedures provide guidelines and expectations for employees' security-related behaviors. Albrechtsen et al. (2020) emphasized the role of security policies and procedures in shaping employees' policy compliance and compliance with security practices. When policies and procedures are effectively communicated, regularly updated, and enforced consistently, they enhance employees' understanding of security requirements and foster a culture of compliance.

Cybersecurity policy compliance campaigns are an essential strategy for mitigating cybersecurity risk. Kifle et al. (2020) highlighted the impact of cybersecurity policy compliance campaigns on employees' behaviors and organizational culture. A positive and inclusive culture fosters a sense of belonging and promotes a high level of employee engagement and commitment (Denison et al., 2021). Through targeted training programs, organizations can enhance employees' understanding of security risks, promote best practices, and empower them to become proactive contributors to organizational security. Establishing effective incident response and reporting mechanisms is crucial for a robust security policy compliance program. Alam and Ahad (2022) emphasized the importance of incident response practices in enhancing employees' policy compliance and prompt reporting of security incidents. By providing

clear guidelines for incident reporting, organizations can encourage employees to actively participate in incident response activities and contribute to the overall security posture.

Organizational culture, policies, and practices can comply with various regulatory requirements and standards that mandate the protection of information, data, and privacy. Organizational culture can demonstrate the commitment and efforts of the organization to enhance its security posture and performance by providing evidence of its security policy compliance training activities and outcomes (Ghazal & Awan, 2022). Organizational policies can adhere to the applicable laws and regulations that govern the collection, processing, and disclosure of information, data, and privacy, such as the EU General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI DSS). Organizational practices can audit and review the effectiveness and efficiency of security policy compliance programs by conducting internal or external assessments, evaluations, or certifications (Bélanger et al., 2017; Best Practices for Implementing a Security Policy compliance Program, 2014; The Benefits of Information Security and Privacy Policy compliance Training Programs, 2019).

Effective communication and policy compliance campaigns are essential for engaging employees in security initiatives. Alabdulatif et al. (2021) explored the factors influencing employees' cybersecurity policy compliance, highlighting the role of communication strategies. Organization leaders can disseminate security-related information, promote best practices, and raise employee policy compliance by leveraging various communication channels, such as emails, newsletters, posters, and workshops. A

flexible and innovative organizational culture and responsive policies and practices empower organizations to navigate challenges and capitalize on opportunities (Kim & Choi, 2021).

Organizational culture, policies, and practices significantly influence the success of security policy compliance programs in organizations. Chen et al. (2022) stated that organizational practices encompass the tangible actions, processes, and systems that support the implementation of policies and reinforce the desired organizational culture. By fostering a positive security culture, implementing clear security policies and procedures, providing comprehensive training and education, establishing effective incident response mechanisms, and employing communication and policy compliance campaigns, organizations can create a culture of security policy compliance among employees. These factors collectively contribute to minimizing cyber risks and protecting organizational assets. A positive and robust organizational culture drives employee engagement, job satisfaction, and overall performance (Denison & Mishra, 2022). Organizational culture, policies, and practices can mitigate cyber threats and reduce human error among employees and stakeholders by influencing their attitudes and behaviors toward security policy compliance programs.

Organizational culture can motivate employees to participate in security policy compliance programs and apply what they learn by providing intrinsic and extrinsic rewards, such as self-efficacy, autonomy, competence, recognition, feedback, or incentives. Organizational policies can regulate employees' access and use of information, data, and resources by implementing appropriate technical and

organizational measures to ensure confidentiality, integrity, availability, and resilience. Organizational practices can test and improve employees' knowledge and skills on security policy compliance topics by providing them with relevant and engaging training, such as fear appeals, gamification techniques, or personalized messages (Boss et al., 2015; Chen & Wang, 2022; Lee & Park, 2023; The Benefits of Information Security and Privacy Policy compliance Training Programs, 2019).

## Transition

In Section 1, I addressed the background of the problem, problem statement, purpose statement, nature of the study, research questions, conceptual framework, and significance of the study. In this study, I will identify and explore effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance. Also, I stated the rationale for choosing a qualitative pragmatic inquiry design and included assumptions, limitations, delimitations, and operational definitions. The literature review included a comprehensive and critical analysis and synthesis of literature related to the conceptual framework, protection motivation theory, along with supporting and contrasting theories.

In Section 2, I provided justification for selecting the qualitative research method and restated the purpose statement. Also, I addressed the role of the researcher in the data collection process, participants in the study, population sampling, and ethical research procedures. Section 3 will include the presentation of findings and how they apply to professional practice. It also included implications for social change, recommendations for further research and reflection on the doctoral study process is provided.

# Section 2: The Project

In this section, I discuss the purpose statement, role of the researcher, participants, research method and design, population and sampling, ethical research, and data collection processes. Analysis of the data and the strategies used to ensure the study's reliability and validity are also presented.

## Purpose Statement

The purpose of this qualitative pragmatic inquiry was to identify and explore effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance. The targeted population consisted of five business leaders of five IT organizations located in the United States who successfully implemented an employee cybersecurity policy compliance training program. This study might contribute to positive social change by mitigating damage from cyberattacks to help business firms provide stable employment to their employees and help consumers to avoid paying for economic costs of cyberattacks.

## Role of the Researcher

As a researcher, strict adherence to all data collection guidelines is imperative. The qualitative approach is employed by researchers to engage in an interpretive methodology aimed at achieving a profound understanding of research phenomena and assessing the perspectives and feedback from study participants (Frost & Bailey-Rodriguez, 2020). Balancing adherence to data collection guidelines while extracting comprehensive information from participants poses a challenge. Thus, the efficacy of the

study hinges upon the precise gathering of data, a goal that I did achieve through meticulous attention to detail.

As an experienced professional with an extensive background in the cybersecurity industry including both mid-level and leadership roles over several years, I have developed a thorough familiarity with cybersecurity policy compliance programs. I do not currently or have previously worked directly with any participants in the study, but it's possible that I might have encountered some of them through my networks. My accumulated experience had equipped me with a distinctive viewpoint, enabling effective communication with participants through the utilization of industry-specific terminology and acronyms. My approach to engaging with participants did prioritize courtesy and cultural sensitivity, fostering an environment conducive to open and concise responses. My ample exposure to cybersecurity policy compliance training was attributed to my involvement in a range of mid-level and leadership positions held within the industry over the course of numerous years.

I did adhere to ethical principles to prevent bias, participant exploitation, and the subjective interpretation of data. According to Braun et al. (2020), acquiring data through participant involvement can present challenges, as individuals might not feel at ease discussing personal matters openly. Researchers can surmount this obstacle by adhering to ethical guidelines and conducting research in an inclusive and respectful manner that safeguards the rights and well-being of study participants (Carter et al., 2021). In this study, my commitment to open and transparent communication, along with collaborative efforts, did foster an environment where participants feel at ease providing confident

responses. According to Wiles et al. (2021), researchers should uphold ethical standards, which encompass transparency, honesty, and the safeguarding of participants' rights, to ensure the impartiality of the study. Although there might exist professional associations with certain participants, I acknowledged the potential for bias and did address it by adhering to the principles outlined in the Belmont Report. The Belmont Report outlines three core ethical principles – respect for individuals, beneficence, and justice – and additionally outlines protective measures for informed consent, risk/benefit evaluation, and participant selection (Khan & Khan, 2020).

To maintain uniformity and minimize potential bias, I employed a consistent interview protocol (see Appendix A), posing identical questions in the same sequence to all participants during the interviews. Additionally, I did apply member checking by providing each participant with an interview summary. I also utilized data saturation to reinforce the study's findings' credibility and validity. The data saturation is reached when the analysis of additional data does not yield new themes or information that was not identified based on the data that had been collected.

A pivotal element of this study involved collecting data through participant interviews, which were facilitated via teleconferencing to minimize disruptions and enhance participant comfort. As indicated by Mackenzie and Knipe (2021), using semistructured interviews enables researchers to pose targeted questions, thus fostering meaningful and purposeful dialogues that allow participants to convey their experiences in their own words. The interview procedures and questions employed in the study are detailed in the interview protocol (see Appendix). The implementation of semistructured

interviews yielded comprehensive participant responses. I documented participants' input and feedback throughout these interviews, utilizing NVivo to discern themes within the data. Braun and Clarke (2021b) elucidated that during qualitative research, NVivo serves as a tool to efficiently conduct thematic analysis through data organization and the identification of themes. The interviews were concluded by summarizing key points highlighted by participants, followed by an opportunity for participants to raise any specific queries they may have by member checking.

## Participants

The target population comprised five IT leaders located in the United States who have effectively implemented a cybersecurity policy compliance program in their organizations. These information technology leaders were senior executives responsible for guiding cybersecurity endeavors within their organizations. To elevate the quality of research data, the inclusion of knowledgeable participants is crucial, as their insights and information can significantly enhance the quality of research findings (Gall et al., 2020). For this study, it was a requisite that these leaders possessed more than 7 years of experience in the information technology industry.

To establish contact with the participants, I utilized purposive sampling, recruiting individuals through my professional network on LinkedIn and ensuring their eligibility aligned with the participation criteria. LinkedIn proved valuable in identifying potential research participants and fostering professional connections (Yadav, 2021). Given my ongoing leadership role in the technology sector, I have cultivated professional relationships over the past 15 years.

Employing a variety of strategies, I fostered a productive rapport with the participants. As highlighted by Tomaszewski et al. (2020), cultivating robust relationships with participants can encourage candid sharing of their experiences and viewpoints, thereby enhancing the quality of the collected data. Each potential participant received communication via LinkedIn and email for follow-up that included an introduction to the study and a consent form requesting their participation by responding affirmatively to the email. Subsequently, participants who expressed their willingness to participate received a calendar invitation for scheduled sessions to conduct the study. This invitation included a copy of the consent form and the participant's confirmation email replying with "I consent." Subsequently, I conducted semistructured interviews and reviewed pertinent organizational documents to garner responses to the research question: What effective strategies do IT leaders of small businesses use to improve employee's cybersecurity policy compliance?

## Research Method and Design

The research method and design of the study was qualitative pragmatic inquiry study. Researchers use the qualitative method to employ an interpretive methodology to gain an in-depth knowledge of research phenomena, which enables researchers to explore phenomena by interacting with the research participants (Frost & Bailey-Rodriguez, 2020). I utilized the qualitative method for this study because I explored the phenomenon in depth. Using the pragmatic inquiry design enables researchers to collect, interpret and compare data collected from numerous participants across multiple sites who observed phenomena in a real-life environment (Saunders et al., 2018).

## Research Method

Researchers have the option to use qualitative, quantitative, or mixed methods in their studies (Saunders et al., 2018). In this study, I selected the qualitative research approach. According to Kelle (2021), utilizing the quantitative method enables researchers to draw from a variety of data sources, including organizational records and interviews, to comprehend the underlying reasoning behind a conceptual framework addressing a specific business issue. Simply, qualitative research is employed by researchers to gain valuable insights into business challenges as perceived from the perspectives of the participants (Williams & Van Ryzin, 2021). The qualitative method serves as an interpretive approach allowing researchers to acquire an in-depth understanding of research phenomena by engaging with study participants (Frost & Bailey-Rodriguez, 2020). For this study, I opted for the qualitative method because it involves direct interaction with participants to capture their viewpoints.

Quantitative researchers employ hypotheses to establish relationships between independent and dependent variables (Saunders et al., 2018). However, the quantitative approach is not suitable for this study since it doesn't involve examining relationships among variables. Mixed-method studies involve a combination of both qualitative and quantitative elements (Yin, 2018). In this case, I did not utilize the mixed method since my study lacked a quantitative component.

## Research Design

For this research, I opted for the pragmatic inquiry design. During the consideration phase for research design options in this qualitative study, a case study,

mini-ethnography, and phenomenology were also contemplated. Utilizing the pragmatic inquiry design allows researchers to gather, interpret, and compare data acquired from various participants across multiple locations, all of whom have observed phenomena in authentic real-life settings (Saunders et al., 2018). I selected the pragmatic inquiry design for my research because I intend to comprehend phenomena through the lens of diverse participants across various sites in authentic real-life contexts.

Employing a case study design empowers researchers to delve into how and what questions, thus facilitating an understanding of the characteristics inherent to the case under investigation (Yin, 2018). Yin (2018) outlined that case studies incorporate four primary strategies: a holistic single case study, a single case study with embedded units, a holistic pragmatic inquiry study, and a pragmatic inquiry study with embedded units. Single case designs are employed when investigating distinctive circumstances within a particular context (Saunders et al., 2018). Yin underscored that single case studies are frequently chosen when testing a well-established theory, particularly in instances where the case is distinctive or longitudinal, involving the evaluation of the same group of individuals across multiple time points.

Researchers adopt a mini-ethnography approach to examine cultures or social environments (Saunders et al., 2018). As I won't be immersing myself in the participants' culture to explore their behaviors, beliefs, and language, the mini ethnographic design wasn't suitable for this study. Similarly, researchers employ a phenomenological design to delve into the lived experiences of study participants (Tomaszewski et al., 2020). However, the phenomenological design wasn't suitable for this study, as my focus

centered on the strategies employed by small business IT leaders to improve employee cybersecurity policy compliance rather than individual lived experiences.

I selected the pragmatic inquiry design for my research because my aim was to comprehensively grasp phenomena through the insights of diverse participants in various settings within real-world contexts. Gaining insights into the practical experiences of strategies employed by IT leaders to enhance employee cybersecurity policy compliance in their organizations could potentially raise policy compliance within the cybersecurity industry. Furthermore, the study might offer insights that could aid in mitigating the impact of cyberattacks, thus contributing to the stability of employment within business firms and assisting consumers in avoiding the economic burdens associated with cyberattacks.

In the process of conducting research, data collection has a point of completion. Data saturation emerges when the collected data ceases to unveil any novel themes (Guest et al., 2020). Essentially, data saturation signifies the point where new information no longer emerges. To guarantee data saturation, I persisted in gathering data through interviews and member checking and public documents until the emergence of fresh themes halted.

## Population and Sampling

The targeted population consisted of five technology leaders situated in the United States, all of whom have successfully implemented an employee cybersecurity policy compliance training program. As per Yin's (2018) guidance, the participant count should offer ample detail and depth to address the research question and objectives

effectively. The number of participants should be large enough to yield comprehensive and meaningful data that can be used to answer the research question and achieve the study's objectives (Smith, 2023). Each of these technology leaders held senior executive roles within organizations, explicitly overseeing information technology functions. A prerequisite for inclusion is that these leaders had more than 7 years in the information technology sector.

The recruitment of participants was executed through purposive sampling. According to Creswell and Creswell (2021), purposive sampling is utilized to gather data from individuals who have experienced a phenomenon, under the assumption that their experiences can reflect the broader population's insights. Through purposive sampling, comprehensive and insightful data can be obtained from participants, offering valuable perspectives on the phenomenon under investigation (Braun & Clarke, 2021a).

The chosen technology leaders for this study held leadership roles in technology within the last 7 years. Leveraging my professional network on LinkedIn, I identified individuals who met the research criteria. The approach involved initiating contact with potential participants via LinkedIn or email, providing them with an introduction to the study alongside a consent form. I used the consent form to solicit their participation and requested an affirmative response through email.

Data saturation transpires when collected data ceases to unveil new themes (Guest et al., 2020). To facilitate the emergence of themes and achieve data saturation, I employed three data collection techniques: conducting interviews through platforms like

Zoom or Microsoft Teams, executing member checking, and scrutinizing public documents. These techniques persisted until data saturation was attained.

To mitigate any potential discomfort stemming from the interview setting that some interviewees may encounter, I opted for Microsoft Teams as the interview platform. This approach ensured that all participants could partake in interviews within an environment they find comfortable, thereby fostering a sense of ease and control. I shared the research questions with participants and clarified any unclear aspects in advance of the interview. Additionally, I used the meeting recording feature on Zoom or Microsoft Teams to capture the interviews, facilitating transcription to my computer post-interview (Parameswaran et al., 2020).

## Ethical Research

To uphold ethical standards in research, it is imperative to secure participants' consent by outlining the researcher's methodologies and ethical guidelines (American Psychological Association, 2020). To achieve this, each potential participant was presented with a consent form. The interview protocol, which is included in the Appendix, served as a comprehensive disclosure document that participants agreed to prior to their engagement in the research. This form delineates the study's purpose, interview procedures, study nature, associated risks and benefits, as well as confidentiality aspects.

Before initiating interviews, prospective participants received an email invitation detailing the introduction, study objectives, eligibility criteria, and an attached informed consent form. This email requested participants to review and acknowledge their

acceptance or refusal to partake electronically by emailing with "I consent." Participants could inform me at any point in the process, in writing or verbally, if they wished to withdraw. I did not offer any incentives to participants as encouragement for participation. To ensure participants' comfort with the research data collection methodology, I adequately informed them beforehand about the approach utilized in the interview protocol.

Confidentiality of study participants is an essential responsibility for researchers (O'Donnell & Ryan, 2021). To ensure confidentiality, participants and their respective organizations were assigned pseudonyms. Leveraging my professional network, I established connections with information technology leaders and asked if they would like to partake in the study. Prior to initiating the research, adherence to confidentiality requirements, outlined in Walden's research guidelines, mandates obtaining a Collaborative Institutional Training Initiative (CITI) certificate.

Preserving participants' rights is paramount, and I will store the data in a secure location within my residence for a duration of 5 years. This data will be stored on a password-protected external hard drive and securely locked within a cabinet. After the lapse of 5 years, all written or recorded data will be eliminated. Throughout the study process, the Institutional Review Board (IRB) mandates unwavering protection of participants. My Walden IRB approval number was 09-08-23-1117675, and I will adhere to the tenets of the *Belmont Report* to ensure the sustained protection of participants' rights. To safeguard participant confidentiality, I used pseudonyms to abstain from

revealing participants' names or any identifiable information concerning them or their respective organizations.

## Data Collection Instruments

In this study, I was the primary instrument for data collection. I employed a combination of semistructured interviews, member checking, and the review of publicly available documents. To gather the requisite data for qualitative pragmatic inquiry, researchers often turn to diverse sources such as interviews, direct observation, and documentation (Fisher, 2021). While the quantitative method, according to Kelle (2021), permits researchers to draw on a variety of data sources, including organizational records and interviews, to comprehend the rationale behind the conceptual framework within a specific business problem, the focus of this study remained on qualitative methods.

The primary research data were gleaned from semistructured interviews, supplemented by secondary data sources encompassing publicly available information. Semistructured interviews hold significant value in qualitative research, allowing for an in-depth exploration of participants and their insights, while member checking enhances data accuracy and comprehensiveness (Creswell & Creswell, 2021). The semistructured interviews were employed to delve into the strategies that small business IT leaders use to improve employee cybersecurity policy compliance.

Open-ended interview questions guided the interviews, with the participants' responses being captured through handwritten notes and audio recordings. The interview protocol, detailed in Appendix A, encompasses the interview questions and the methodologies employed during the interview sessions. Interview protocols serve to

maintain the quality and consistency of data collection while enhancing the efficiency of the interview process (Safdar & Chua, 2021). The interview protocol served as a guide, directing the implementation of open-ended interviews and maintaining consistency across interview flow, participant rights, interviewer guidelines, and the interview timeline.

Furthermore, for the study's secondary data collection approach, I incorporated publicly available organizational documentation sourced from organizational websites. The documentation such as the organization mission statement, reports and policy and procedure outlining the rules and regulations that the organization follows. This supplementary method provided additional insights into the research question by drawing on organizational documentation and reinforcing the research themes with corroborative evidence. To ensure data saturation, data collection persisted until no new themes emerged.

Yin (2018) identified factors such as generalizations, bias, and poor recall as potential threats to the validity and reliability of research findings, potentially compromising the accuracy and robustness of the obtained data. It is essential to subject the interview protocols and research questions to evaluation by qualified professionals in the field to ensure their reliability and validity (Minichiello et al., 2021). Walden's committee members reviewed the interview questions to ensure alignment with the research questions, further ensuring validity and reliability. Moreover, member checking was used by sending participants a follow-up email containing a summary of their interview responses, enabling them to verify the accuracy and completeness of their

input. Lietz and Zayas (2021) advocate for member checking as an effective approach to bolster the reliability and validity of qualitative research, as it empowers participants to corroborate and validate their responses.

## Data Collection Technique

The research question addressed by this study was: What effective strategies do IT leaders of small businesses use to improve employee's cybersecurity policy compliance? In the pursuit of data collection essential for qualitative pragmatic inquiry, researchers commonly draw from various sources such as interviews, direct observation, and documentation (Fisher, 2021). The combination of diverse data sources to corroborate study findings is advocated as it provides a more credible and well-rounded perspective compared to relying solely on one viewpoint (Alberti-Alhtaybat et al., 2019). The data collection approach adopted here encompassed open-ended interviews, followed by member checking through email correspondence, and the review of publicly accessible documentation.

Interviews are a widely utilized data collection technique in qualitative research, offering a nuanced understanding of participants' experiences, perspectives, and insights. The advantages of using interviews as a methodological approach include gaining rich and in-depth information directly from participants. The richness of the interview methodology can provide valuable insights into complex phenomena that might be missed by quantitative methods alone (Smith & Johnson, 2022). The flexibility of interviews enables researchers to adapt their questions and probes based on participants' responses, uncovering unexpected avenues of exploration (Brown et al., 2020).

Interviews provide the opportunity to understand participants' experiences within their personal and social contexts, shedding light on the interplay between individual and societal factors (Williams, 2021).

The disadvantages include subjectivity from personal biases, beliefs, and experiences of the researcher that can influence the research process. The researchers' interpretations and biases inherently influence interviews, potentially introducing subjectivity into data analysis (Jones, 2019). Interviews can be time and resource-intensive to conduct, transcribe, and analyze. Conducting interviews requires substantial time and resources, from participant recruitment to transcription and analysis, making it less feasible for large-scale studies (Davis et al., 2023). Some participants may feel uncomfortable discussing sensitive topics in face-to-face interviews, leading to the potential withholding of information or socially desirable responses (Martinelli, 2020).

To maintain uniformity across participants, the interview protocol (see Appendix A) will be strictly adhered to. The interviews involved introducing the study, presenting the research question, and posing eight open-ended queries. Subsequently, a follow-up email was dispatched for member checking, allowing participants to review a summary of their interview responses and provide additional insights if necessary. To ensure data validity, interviews will be conducted with five participants from five organizations. Interview protocols are recognized for their ability to ensure consistent, high-quality data collection and enhance interview efficiency (Safdar & Chua, 2021). In the context of this study, the interview protocol (see Appendix A) outlines the questions and methodologies employed during the interviews. These interviews were conducted through platforms like

Microsoft Teams or Zoom, with the recordings transcribed into a word document. Following the interviews, member checking was performed, and publicly accessible organizational documentation was reviewed to ensure the reliability and validity of the participants' responses.

Member checking, as suggested by Lietz and Zayas (2021), is a robust method for enhancing the credibility of qualitative research by enabling participants to review and refine their experiences. To facilitate this process, a follow-up email containing a summary of the responses was sent, allowing participants to confirm the accuracy and completeness of their inputs. This member checking exercise empowered participants to ensure that their reflections align with their concepts regarding the interview questions.

In line with Mackenzie and Knipe's recommendation (2020), combining multiple data sources amplifies triangulation, thereby bolstering result accuracy and reliability. Pinnock et al. (2021) have also underscored that employing various data sources in data collection techniques enhances study validity and dependability. The interviews and member checking facilitated deeper participant insights during interviews, though potential drawbacks, such as the risk of eroding participant trust and misinterpretation of responses, warrant consideration (Zhao et al., 2021).

Additionally, the review of publicly accessible documentation allowed for the collection of additional data without imposing excessive demands on participants' time. Nevertheless, this approach has limitations, such as potential data obsolescence and information incompleteness.

## Data Organization Technique

To ensure effective data organization and structured coding, meticulous planning and data management strategies are indispensable (Chen & Boore, 2021). Implementation of standardized labeling and cataloging systems aids in enhancing data reliability and sharing across studies (Gallagher et al., 2021). Each participant's information was meticulously labeled, and for confidentiality, each was assigned a unique character and/or number referenced throughout the study. All notes and recordings were linked to participants through their unique identifiers. Compliance with Walden University's research guidelines necessitates obtaining a CITI certificate, thereby reinforcing the need for participants' confidentiality.

The electronic and hard copies of the data will be stored securely for a 5-year period to safeguard participants' information. At the conclusion of this period, any written or recorded data will be securely destroyed, and where applicable, external hard drives will be wiped clean. The IRB mandates continuous protection of participants' rights throughout the study. The final doctoral manuscript will bear the Walden IRB approval number, while adherence to the requirements outlined in the *Belmont Report* further ensured participants' rights were protected throughout the research journey.

## Data Analysis

Triangulation serves as a fundamental tool for researchers to scrutinize data validity and reliability (Fusch et al., 2018). Methodological, investigator, theory, and data source triangulation are strategies utilized to ensure the dependability and authenticity of research. In this study, I employed methodological triangulation to enhance data

comprehension. Methodological triangulation enables researchers to explore phenomena from diverse angles, often involving multiple data sources like organizational documents and interviews (Fusch et al., 2018). Employing data triangulation, which involves multiple evidence sources, reinforces the credibility and trustworthiness of doctoral research. Hancock et al. (2021) described case study research as characterized by its richness and groundedness in a diverse array of data sources.

Collecting data from various sources corroborates the reliability of data and bolsters the overall credibility of doctoral research, unlike relying solely on a single source. My data collection approach encompassed interviews, member checking, and publicly available organizational documentation, aimed at facilitating efficiency and productivity, fostering methodological triangulation for this study. To guide the interview process, I utilized open-ended interview questions (see Appendix A) that delved into strategies employed by IT leaders to enhance employee cybersecurity policy compliance. Following interviews, member checking was conducted to validate and solidify the authenticity of participants' responses, allowing them to provide additional insights or clarify points not fully covered during the interview (Saunders et al., 2018). As an additional source of data, I gathered secondary information from publicly available organizational documentation on their respective websites to provide further support for identified themes. Data collection persisted until no new themes surfaced, ensuring data saturation.

Following Yin's (2018) approach, data analysis involves utilizing software for data organization, coding, interpretation, and conclusion drawing. The organization of

coding aligned with my research questions and interview inquiries. According to Dalkin et al. (2021), researchers structure data based on their research inquiries and then categorize and arrange codes and concepts according to each interview question and other data sources, revealing patterns and themes. For this research, NVivo 12 was employed to assess the coded data—a qualitative data analysis software acknowledged for aiding researchers in uncovering and coding concepts (Dalkin et al., 2021).

To address the research question, I followed Yin's (2009) five-step sequential analysis methodology. The first step of the methodology involves collecting and organizing all the data that has been collected during the research study. I did this by entering all of my transcripts, member checked documents and publicly available organizational documents into NVivo. The second step is to disassemble the data by breaking down the data into smaller, more manageable pieces to make it easier to identify patterns and themes. I did this by reviewing the data to identify themes. The third step is to reassemble the data which involves putting the data back together in a way that makes sense. I did this by describing each theme, counting the number of occurrences of each, and identifying illustrative examples of each. The fourth step is interpretation which helps to make the research findings more practical and applicable. I did this by using the PMT theoretical framework to compare and contrast the findings to assess the validity and reliability. The fifth and final step is conclusions that are based on the evidence that has been presented in the study and must be clear, concise, and easy to understand. I did this by summarizing the main findings and implications of the case study research.

Data analysis will occur using NVivo software to identify themes, with thematic analysis serving as the principal method for theme identification. Throughout the data organization process, an audit trail was established to capture and document unique and intriguing topics encountered during data collection, guiding coding and rationale. Afshar and Ahmadvand (2022) highlighted that thematic analysis facilitates a systematic and comprehensive examination of data, breaking down narrative materials into distinct content groups with descriptive treatments to unveil connections within the study's context. Emerging themes were then aligned with the study's conceptual framework, the protection motivation theory, and existing literature to identify strategies employed by small business IT leaders to enhance employee cybersecurity policy compliance. To validate transcription and ensure triangulation, member checking was used to verify data analysis accuracy, while publicly accessible organizational documentation served to validate analyzed data and potentially uncover new themes.

## Reliability and Validity

The quality of doctoral research is intricately tied to the concepts of reliability and validity, underscoring their fundamental significance in ensuring well-executed and credible research. As Yin (2018) emphasized, aspects such as data collection, methodology, strategic approach, and a trustworthy philosophical foundation constitute pivotal elements of proficient research. Reliability and validity serve to uphold the integrity of doctoral research endeavors and enhance the overall credibility of the work. Notably, numerous challenges related to data quality could potentially cast a negative influence on the trajectory of a doctoral research study. Saunders et al. (2018) expounded

on the notion that improper utilization of research methods and tools might undermine the validity and reliability of data pertinent to the research objectives. Johnson et al. (2020) corroborated this by highlighting the considerable influence of research methodology on the eventual findings and conclusions drawn. In essence, the quality of data stands as a critical pillar in the pursuit of conducting doctoral research that is both robust and credible.

The establishment of reliability and validity hinges upon the meticulous collection of data. To accomplish this, I counteracted potential pitfalls of participant and researcher error and bias by meticulously transcribing and accurately documenting responses and findings. Additional measures included subjecting the data to member checking and ensuring the possibility of replicating the study, all of which collectively work towards enhancing the reliability and validity of the research.

**Reliability**

Data quality is essential for conducting doctoral research that is trustworthy and reliable. According to Saunders et al. (2018), reliability and dependability are attained by employing member checking, reviewing transcripts, and utilizing triangulation. Lietz and Zayas (2021) suggested that member checking is regarded as a potent approach for augmenting credibility. Dependability can be ensured through the utilization of audit trails and triangulation methods. Subsequent to the interview, I performed member checking by forwarding the summary to the participants to validate that their responses have been accurately and comprehensively represented, thus confirming the interpretive accuracy. Pinnock et al. (2021) also pointed out that the utilization of multiple data

sources in data collection techniques enhances the study's reliability and dependability. Researchers employ methodological triangulation to investigate phenomena from various angles, utilizing data gathering and analysis methods such as examining organizational documents and conducting interviews (Denzin & Lincoln, 2011). To enhance the reliability and dependability of the interview process, the interview questions were reviewed by Walden's committee members to ensure alignment with the research questions. I incorporated multiple strategies to ensure reliability and attain data saturation, including participant validation, expert verification of interview questions, adherence to participant interview protocols (see Appendix A), and the implementation of methodological triangulation.

**Validity**

Ensuring validity is a crucial element of qualitative research, establishing the credibility and believability of results from the perspective of the research participants. To uphold data validity, researchers utilize techniques like member checking and the adoption of diverse data collection and analysis methods.

The validity of qualitative research relies on key principles of data collection, encompassing aspects such as credibility, confirmability, and the transferability of findings (Yadav, 2021). In this study, I established validity by attaining data saturation through interviews, document analysis, member checking, and the utilization of multiple methods. Additionally, data will be collected from interviews, publicly accessible records, and member checking to ensure validity. Methodological triangulation was employed for data analysis and presentation, continuing until no new themes emerged

from the interviews. The achievement of data saturation guarantees the credibility, confirmability, and transferability of the study's findings.

**Credibility**

In qualitative research, the foundation of credibility must revolve around the participant's viewpoint. Credibility challenges often stem from biases, a prevalent concern. Those engaged in doctoral research should diligently avoid introducing personal biases into their work. Managing biases is of utmost importance, and can be achieved through adherence to interview protocols, implementation of member checking, collection of data from diverse sources, and meticulous documentation (Saunders et al., 2018). Recognizing the significance of data quality in a doctoral study and mitigating biases will cultivate reputable doctoral research. Given this standpoint, qualitative researchers aim to depict or comprehend the phenomena of interest through the participant's viewpoint, rendering them the sole legitimate assessors of result credibility. Strategies such as interview protocols, triangulation, member checking, and data saturation will be employed to ensure this study's credibility.

**Transferability**

Transferability represents another vital facet of qualitative research, and researchers can amplify transferability by upholding the research design as well as interview and protocol standards. Transferability represents a vital facet of qualitative research, and researchers can amplify transferability by upholding the research design as well as interview and protocol standards (Elmusharaf et al., 2021). Furthermore, as Saunders et al. (2018) suggested, researchers are advised to incorporate diverse data

sources to attain data saturation, thereby augmenting the transferability of the outcomes. For my research design, I adopted the pragmatic inquiry method, adhered to the interview protocols (Appendix A), and gathered data from various sources to achieve data saturation, reinforcing my findings' transferability.

**Confirmability**

Ultimately, confirmability pertains to the degree to which external sources could verify or support findings. According to Yin (2018), enhancing confirmability is attainable through member checking, involving the accurate presentation of participants' responses with the researcher's interpretations while minimizing biases and potential lapses in memory. Additionally, to derive interpretations from results, researchers employ methodological triangulation to validate diverse data sources (Fusch et al., 2018). To uphold the confirmability of this study, I applied member checking and methodological triangulation to ensure the extent to which the outcomes could be validated or substantiated by external parties.

**Data Saturation**

In qualitative studies, researchers consider that data saturation is critical for collecting adequate and high-quality data to support the study and demonstrate content validity. Data saturation occurs when the data collected does not reveal any new themes (Guest et al., 2020). According to Yin (2018), researchers are unaware of reaching saturation until they analyze the obtained data. I ensured that I achieved data saturation by analyzing the data collected to ensure the absence of new data and topics. In addition, I obtained sufficient data to address the research question through interviews,

documentation, member checking, and methodological triangulation until no new information emerged.

## Transition and Summary

In Section 2 of this qualitative study, I outlined the role of the researcher, the participants, the research method, the research design, the population and sampling, foundations of ethical research, data collection instruments, data collection technique, data organization technique, data analysis, and reliability and validity. Additionally, Section 2 includes particulars on the role of the researcher, participants, research method and design, population and sampling, and ethical research. Section 2 also include the process for data collection, the qualitative data analysis software used in the data analysis process, and the data validation for the study, which explores effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance. Section 3 will contain the presentation of findings, the application to professional practice, implications for social change, recommendations for actions, suggestions for further research, reflections, and a conclusion.

Section 3: Application to Professional Practice and Implications for Change

## Introduction

The purpose of this qualitative pragmatic inquiry was to identify and explore effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance to help business firms provide stable employment to their employees and help consumers to avoid paying for economic costs of cyberattacks. Data were obtained through semistructured interviews with technology leaders in the United States and by accessing publicly available information on the companies' websites. Each participant was sent a consent form via email, which they examined and acknowledged by responding with the phrase, "I consent." The consent form explained the purpose of the study and how participants could withdraw at any time. Thematic analysis was employed in this study to discern patterns and themes from the data. Three themes emerged from data analysis: (a) threat appraisal strategy; (b) self-efficacy strategy; and (c) response efficacy strategy. The protection motivation theory grounded this study. This section includes the presentation of the findings, the study's application to professional practice, implications for social change, suggestions for action, recommendations for further research, reflections, and conclusions.

## Presentation of the Findings

Five experienced technology leaders with a background of 7 years or more in technology leadership roles from five prominent organizations took part in this study. The research was guided by a central question: What effective strategies do IT leaders of small businesses use to improve employee's cybersecurity policy compliance?

Participants were asked to respond to eight open-ended interview questions (see Appendix) to provide detailed insights into the strategies aimed at enhancing employee cybersecurity policy compliance training programs. Each technology leader who took part in these interviews shared their experiences related to the implementation of these strategies. Participant demographics are summarized in Table 2.

**Table 2**

*Participants Demographic Summary*

| Participants | Years of experience | Organization | Designation |
|---|---|---|---|
| P1 | 18 | Corporate | Executive |
| P2 | 24 | Government | Executive |
| P3 | 25 | Private | Owner |
| P4 | 30 | Government | Executive |
| P5 | 41 | Government | Executive |

P1 is a top-level executive who oversees the technology, risk, and compliance in a large insurance company. P1 is a global traveler with a passion for culture and making the world a better place. PI holds a doctorate in business administration and various information security certifications.

P2 was a software programmer for a corporate organization before working her way to an executive position as the head of the IT group of her current organization. P2 enjoys reading, spending time with the family, exercising, and watching football.

P3 was a practicing cybersecurity profession and owner of a cybersecurity consulting company that provides information technology managed services that specialize in providing services and solutions to help businesses adhere to cybersecurity standards and regulations, ensuring their systems and data are secure and in compliance with industry or legal requirements. P3 is a cybersecurity coach in IT governance of

enterprises conducting global training on cybersecurity, governance, and risk management.

P4's career started in an employee benefit department using computers to automate processes. P4 was fascinated with how computers processes information's within milliseconds and the supporting infrastructure. P4 enjoys long distance biking and spending time with the grandchildren.

P5 is an award-winning executive with IT experience that can be traced to her college days. P5 has been married with children for more than 43 years. P5's IT career started with the corporate oil and gas industry and banking industry for 20 years before transitioning to a leadership role at a government enterprise 21 years ago. P5 started working as a senior system analyst and project management.

During the third interview, it became apparent that data saturation had been reached, a conclusion confirmed during the fourth and fifth interview. Follow-up interviews questions and member checking were conducted to review and interpret the collected data. These member checks did not yield any new information that could have altered the study findings.

I utilized Yin's (2009) five-step approach to qualitative data analysis to scrutinize the textual data gathered from participant interviews and the examination of publicly available information from the organizations' websites. This process involved compiling, deconstructing, and reconstructing data, deciphering data meanings, and drawing conclusions from the results. Initially, data were compiled for organizational purposes and then deconstructed to eliminate invariant themes related to the phenomenon.

Subsequently, the data were reassembled, focusing on core themes. Finally, I cross-checked patterns against interview transcripts. Following the thematic analysis, I meticulously examined emerging themes, comparing them with the existing literature, conceptual framework, organizational documents, transcripts, and NVivo results. To maintain participant confidentiality, pseudonyms were used. For instance, participants were labeled as P1 etc., and transcripts were coded similarly.

The data collection process involved recording participant interviews on Teams, automated transcription, and comparing participant responses with publicly available information on organizational websites. Initially, I transcribed the interviews using Microsoft Word, meticulously reviewed and edited the transcriptions, and highlighted pertinent information relevant to the guiding research question. These transcripts were then imported into NVivo for organization, analysis, and data coding. Additionally, I maintained an audit trail to organize my thoughts about the coded data during this process. To confirm emergent themes, I conducted a word search query in NVivo, comparing them with themes from participant transcripts and grouping coded data based on these emergent themes. Three themes emerged from data analysis: (a) threat appraisal strategy; (b) self-efficacy strategy; and (c) response efficacy strategy (see Table 3).

**Table 3**

*Emergent Themes from Data Analysis*

| | Threat appraisal | Self-efficacy | Response efficacy |
|---|---|---|---|
| Number of times the participant mentioned this theme | 17 | 14 | 13 |

## Theme 1: Threat Appraisal Strategy

Theme 1, threat appraisal strategy, refers to strategies associated with the individual belief that employees can successfully take action to protect themselves from a threat. Executive leadership support is critical in fostering employees' self-efficacy and encouraging compliance with cybersecurity policies. Executives should communicate openly and transparently about the cybersecurity threats faced by the organization. Regular updates, emails, or town hall meetings can inform employees about the latest cybersecurity risks, incidents in the industry, and the potential impact on the organization. When executives demonstrate their commitment to cybersecurity by designing and enforcing strong policies and procedures, employees are more likely to believe they have the resources and support they need to protect themselves and the organization from cyber threats. Threat appraisal strategy was the most frequently mentioned among participants, with 17 references during interviews.

Participants consistently highlighted the significance of threat appraisal strategies in designing and enforcing policies and procedures. Executive leaders must demonstrate their commitment to cybersecurity by following security policies themselves and by communicating the importance of cybersecurity to all employees. The active participation

of employees in security policy compliance programs is crucial, and this can be facilitated by strong leadership support and effective communication (Patel, 2022). P1 shared the importance of executive leadership in developing and implementing a cybersecurity policy that is clear, concise, and easy to understand. Further, P2 supported the notion that executive leaders can help ensure that their employees are aware of cyber threats and know how to protect themselves, which can significantly reduce the organization's risk of a cyber-attack. P3 reinforced the importance of making sure that the executive leaders communicate the importance of cybersecurity to all employees and by rewarding employees for following cybersecurity best practices.

P4 said that "executive leadership's role in employee cybersecurity compliance is critical because employees are often the weakest link in the cybersecurity chain." Kim and Park (2020) underscored the positive influence of leadership support on employees' adherence to policies and behavior, underscoring the importance of organizational dedication to cybersecurity. P1 shared that "organizational commitment to cybersecurity is essential for creating a culture where employees feel supported and motivated to protect the organization from cyber threats. Indeed, our entire leadership is well appraised of our cybersecurity program and associated policies." P3 gave an example on how leadership support and implementing of policies and procedure:

> I implemented what's called a Change Control Board. So, every time somebody has to change requests, meaning something touching production, I have instituted a policy that cybersecurity must vet that fix. So, I have taken a stance where I have prioritized cybersecurity as being our top dog and making sure that nothing

> gets passed or done without the cybersecurity assessment and okay of cybersecurity So, I have passed the cybersecurity sniff test. Then I'm okay with us moving forward with it, so I've just shown everybody that cybersecurity is important by the actions that I've taken in not allowing us to do certain things without them vetting it, and I think that has helped tremendously.

The participants indicated that it's crucial for the executive leadership to set the tone and culture for cybersecurity. When security is given priority by leaders, its importance is communicated effectively, and resources are allocated appropriately, employees tend to recognize security as a priority and engage actively in security policy compliance programs (Albrechtsen et al., 2020). P4 said,

> If you have your CEO at the end of every meeting, say remember, it is your job to protect us from cybersecurity attacks. Don't click on that link without being sure if in doubt sends it to the IT security team. You know, if you did those type of things that would really help the culture. It's from the top.

The support from leadership and effective communication are crucial factors that motivate employees to comply with security policies and actively participate in security policy compliance programs (Ghani et al., 2021). P5 elaborated on executive leadership support:

> Certainly, our leaders play a vital role in shaping our organization's cybersecurity framework. Their ability to establish a clear vision for cybersecurity and emphasize its importance creates a strong foundation. Through effective communication, our leaders ensure that every employee comprehends the

significance of complying with security protocols. Additionally, their involvement in the development and implementation of cybersecurity policies is instrumental. This ensures that the policies align with our organizational objectives and meet industry standards. When our policies are transparently communicated and well-aligned with our goals, employees are more likely to adhere to them, fostering a secure environment for our organization."

P5 explained further that

We've worked with the executive leadership of our organization to ensure that the awareness training was taken seriously and that it is required of everyone. Our senior management and the executive team, etcetera have gotten behind IT and the cybersecurity team to support those efforts. And so, although we have, you know, a handful, and actually this last time, very few very little oppositions to taking the training after you failed a phishing attempt. And so yeah, that was the greatest challenge that we had and the way that that was. You know, we kind of alleviated that issue and that challenge was the work that we've done with the executive team and our executive leader to make it certain that this training was no longer considered to be non-mandatory to a mandatory.

P2 stated that

Certainly, our executive leaders have been proactive in ensuring our employees are well-informed about cybersecurity threats and best practices through regular training programs. We firmly believe that educated employees are more likely to comply with security protocols, enhancing our overall cybersecurity posture. In

> terms of accountability, our executive leadership takes a hands-on approach. They enforce compliance by implementing consequences for non-compliance and, equally importantly, recognize and reward those who consistently adhere to our security policies. This approach not only instills a sense of responsibility among employees but also fosters a culture of cybersecurity awareness. Furthermore, our executive leaders are actively involved in the ongoing monitoring of cybersecurity compliance metrics.

P1 expressed that

> Our IT department provides regular updates to the leadership on a quarterly basis. This data-driven approach allows our leaders to analyze the current state of compliance, identify areas of improvement, and adjust our strategies accordingly. By doing so, we ensure that our organization remains resilient and adaptive against the ever-evolving landscape of cyber threats.

P2 emphasized the importance of executive leadership support: “You know, back up support from the management leadership. All of those things, you know, monitoring, having someone looking at the logs of different things on a daily basis and taking actions on those are probably the key things.” An organization’s executive leadership is pivotal in shaping and maintaining employee cybersecurity policy compliance. Furthermore, the examination of publicly accessible organizational data reinforced the emerging theme of leadership support in guaranteeing employees’ compliance with cybersecurity policies. For instance, a participant’s organization had a dedicated webpage on its website showcasing board-approved policies and procedures.

**Theme 2: Self-Efficacy Strategy**

Theme 2, Self-efficacy strategy, refers to strategies associated with the individual perception of the severity and vulnerability associated with a threat. Self-efficacy in PMT involves creating awareness about the severity and vulnerability of cybersecurity threats. The strategy includes regularly communicating real-world examples of cybersecurity breaches and their consequences, both within and outside the organization. Sharing relevant news articles, case studies, or internal incident reports can help employees understand the severity of potential threats and the actual impact of non-compliance. Through training, employees become aware of the severity of these threats (e.g., financial loss, identity theft) and their vulnerability to such attacks. By understanding the seriousness of these threats, individuals are more likely to be motivated to engage in protective behaviors. Self-efficacy strategy became evident as the second most frequently mentioned topic, appearing in 14 participant comments during the interviews.

The participants emphasized the importance of self-efficacy strategy in the context of cybersecurity awareness training and phishing simulation programs. According to P4,

> So, when new employees start, there's a whole orientation they cook through and it's in you over the years, I think when I started, it was one day, then it went to three or four days. Part of that even when I did it, it was one day part of it was cybersecurity awareness and they spent some time, going through what is expected, how the bad actors act, and how you can spot things that that don't seem right.

P1 agreed with P4 on introducing cybersecurity awareness as part of new employee onboarding process. P1 elaborated on cybersecurity awareness training:

> I think right from the door once new employees come in as part of the onboarding process, they're getting the cybersecurity training and the annual training that's also creates awareness also, you know, the phishing campaign, you fall for it, you are required to retrain employees on new risks and threats.

P2 provided an insight into the types of cybersecurity awareness training scenarios: "So we have an educational course that everybody is required to take and it's about an hour training session, maybe 45 minutes where you're going through different scenarios and slides and learning about different and cybersecurity scenarios." P3 further stated,

> In my experience, when employees are well-informed about the cyber threats they might encounter and possess the knowledge to protect themselves, they tend to adhere more closely to cybersecurity policies. This heightened awareness significantly contributes to reducing our organization's vulnerability to potential cyber-attacks. It underscores the importance of fostering a culture of cybersecurity awareness among all staff members, ultimately enhancing our overall security posture.

P5 explained that

> Our cybersecurity awareness training plays a crucial role in educating employees about various cyber threats and methods to safeguard both themselves and the organization. The training program includes comprehensive information on

> different types of cyber threats, empowering employees with the knowledge necessary to recognize and respond effectively to these risks. Our current cybersecurity awareness training strategy is multifaceted. It involves annual training sessions, periodic dissemination of informative news snippets, phishing simulation exercises, and an annual Cybersecurity Month newsletter. Through these initiatives, we aim to keep our employees well-informed, alert, and proactive in the face of evolving cyber threats. By combining these educational efforts, we create a robust awareness framework that contributes significantly to our overall cybersecurity resilience.

All the participants cited the advantages of implementing a cybersecurity awareness and phishing simulation program. P4 stated that "cybersecurity awareness training and phishing simulation are integral components of an organization's strategy to enhance employees' understanding, behavior, and compliance with cybersecurity policies, ultimately bolstering the organization's security against evolving cyber threats." P3 agreed with P4:

> Cybersecurity awareness training and phishing simulations play a pivotal role in cultivating a culture of cybersecurity awareness within our organization. Through these initiatives, employees grasp the shared responsibility of upholding security, fostering mutual vigilance, and ensuring compliance with policies. Moreover, these programs highlight the significance of individual actions in preserving our organization's security posture. They promote a culture of skepticism and caution, encouraging employees to approach potential threats with heightened awareness

> and proactive measures. This collective effort significantly enhances our overall resilience against cybersecurity risks.

P1 said, “Employees are more likely to follow cybersecurity policies if they understand the importance of cybersecurity and the risks of non-compliance.” P2 in support stated that “We noticed employees are more likely to be able to identify and avoid cyber threats if they have been trained on how to do so. That’s why we added phishing simulation.” P4 added that “Our employees are more likely to comply with cybersecurity policies if they have the skills and knowledge they need to do so.” P5 added a similar comment: “we are more likely to comply with cybersecurity policies if they have the skills and knowledge they need to do so.” All participants stressed the importance of utilizing various forms cybersecurity training and delivery. P5 commented that

> Certainly, cybersecurity awareness training and phishing simulations are instrumental in fostering a culture of cybersecurity awareness and compliance within our organization. By equipping employees with the knowledge and skills to recognize and respond to cyber threats, these initiatives empower our workforce to actively contribute to our overall security posture. This heightened awareness not only encourages adherence to policies but also promotes a proactive and vigilant approach toward cybersecurity. Through these efforts, we strengthen our organization’s resilience against potential cyber risks and threats.

Overall, cybersecurity awareness training and phishing simulations are essential for organizations that want to improve employee compliance with cybersecurity policies and reduce their risk of a cyber-attack. P5 added that

> By providing employees with these understandings, skills, and knowledge, cybersecurity awareness training and phishing simulations empower our workforce to adhere to cybersecurity policies proactively. This strengthens our organizational defenses and creates a security-aware culture that is resilient against evolving cyber threats.

P1 stated that

> Cybersecurity awareness training and phishing simulations are essential components in enhancing our employees' compliance with cybersecurity policies. They serve as valuable tools by emphasizing the critical significance of cybersecurity and the potential consequences of non-compliance. Employees gain insight into the broader impact of their actions on organizational security.

P3 stated, "So, people should be encouraged to have cybersecurity education because when they have that type of education, it makes it their own cybersecurity process." Cybersecurity awareness training and phishing simulations are essential components in enhancing employees' compliance with cybersecurity policies. cybersecurity awareness program serves as valuable tools by helping employees to identify and avoid threats. Through cybersecurity awareness training and phishing simulations, employees learn to recognize various cyber threats, enabling them to identify suspicious activities and avoid falling victim to phishing attempts or other malicious

activities. Examining the companies' websites revealed information that offered additional supportive evidence for this theme. For instance, one website showcased a prominent cybersecurity awareness training organization as an active partner. This fosters a deeper comprehension and dedication to upholding a secure work environment.

**Theme 3: Response Efficacy Strategy**

Theme 3, response efficacy strategy, comprises of strategies associated with the individual's belief that they have the resources and skills to take effective action to protect themselves from a threat. Investing in robust managed technology solutions that provide comprehensive security coverage, including antivirus software, firewalls, intrusion detection systems, and encryption tools. Ensuring that employees have access to state-of-the-art security tools promotes belief in the effectiveness of these solutions. Managed technology solutions can help organizations to improve response efficacy by providing them with the ability to detect, respond to, and recover from cyber-attacks. Response efficacy strategy involves the deployment of monitoring tools, and managed technology solutions.

The theme surfaced as the third most frequently discussed topic, being mentioned 13 times in participant interviews. response efficacy strategy directly aligns with my conceptual framework, PMT, because it is one of the PMT constructs. The participants emphasized the importance of deployment of monitoring tools and managed technology. Organizational leaders are responsible for providing employees with access to essential training, tools, and technologies to improve their security knowledge and skills, as emphasized by Khan et al. (2021).

P1 explained that “we have a lot of network tools that monitor policy enforcement, such as when you download malware, it can block it, or you are visiting social media sites that you are not supposed to visit, like going into essential media.” P2 said,

> Deployment of monitoring tools indeed plays a pivotal role in improving our employees’ policy compliance. By providing our cybersecurity team with real-time tracking capabilities over employees’ digital activities, we can promptly identify any policy violations. This instant oversight serves as a powerful deterrent, motivating employees to adhere to policies and ensuring a more secure digital environment within our organization.

P3 elaborated on the significance of monitoring tools and managed technology solution:

> We opted for a managed service provider to support us in enforcing policies effectively. Through this partnership, we receive automated alerts and notifications whenever policies are violated, allowing for swift corrective actions to be taken. This proactive approach ensures that our established guidelines are consistently followed by employees, maintaining a secure and compliant work environment.

All the participants agreed that the monitoring of policy violations is a crucial strategy to ensure employee policy compliance.” P4 stated that

> The biggest tool we have is the firewall and enforcing it and allowing people to do certain things. There we could also use access control lists. And then of course, you know the access control as to what systems you’re allowed to access, what

> systems you can access without multifactor authentication of what systems you can access with multi factor authentication.

P4 further stated that

> You need to partner with the vendor that you get your equipment from or something else you know, make sure that your equipment is patched. Make sure that there's an antivirus on it. Make sure that you do have a firewall and that it is updated and all those things you know, if you do all that, that's a pretty good pretty good start. It's not perfect, but it's pretty good.

P5 stated that "part of our cybersecurity activities includes ongoing monitoring of employees' activities within our organization using tools and managed service systems in handling of the data sharing and how they have some ownership with it." P5 also expressed that "depending on how you're sharing with from transit from internal to external, or from, internal to internal on both ends where there's a private information being shared that there is insurance that there is appropriate data protection." P1 and P5 agreed that monitoring tools and managed technology services help detect suspicious behavior or potential security threats, allowing organizations to address issues before they escalate. P2 agreed that "timely intervention minimizes the risk of policy breaches and data breaches." P2 explained in depth on how the leadership utilize managed services:

> Both monitoring tools and managed technology solutions are instrumental in helping our organization meet regulatory requirements. These tools ensure that our policies align with industry standards, enabling us to conduct regular audits and compliance checks effectively. This proactive approach ensures that we

> maintain a high level of adherence to regulations and industry norms, promoting a secure and compliant operational environment. So, our monitoring tools and managed technology solutions offer comprehensive security solutions, such as firewall management, intrusion detection, and regular software updates.

P3 stated that "we utilize various monitoring tools to track employee access to sensitive data, employee use of unauthorized software, and employee visits to malicious websites. P3 further stated that "it's a deterrence for employees knowing that we are monitoring their online activities in case they violate any of the cybersecurity policy." P5 expressed that "monitoring tools are essential to ensure employee compliance as the senior leadership can take appropriate corrective action such ad providing addition training, performance improvement, and possible employment termination." P4 shared that "we employed managed technology solutions that help the department respond to cybersecurity incidents more quickly and effectively. This helps to reduce the damage caused by cybersecurity incidents by acting promptly." P4 said,

> We have opted to outsource our incident management and the monitoring managed program as a strategic step to enhance employee compliance with cybersecurity policies. This involves utilizing a web filtering solution to block access to malicious websites and phishing sites. Additionally, we employ an email filtering solution to prevent phishing emails and spam from reaching employees' inboxes, ensuring a safer communication environment. Moreover, we have implemented a data loss prevention system, which adds an extra layer of security by monitoring and controlling data transfers to prevent sensitive information from

> leaving the organization inadvertently. We utilize a managed security information and event management (SIEM) solution to bolster these efforts. This SIEM system allows us to monitor and analyze security logs for any suspicious activities, providing valuable insights. Furthermore, employees have access to a managed security service provider (MSSP) for assistance with cybersecurity incidents. This collaboration ensures a proactive approach to security and provides employees with the necessary support and expertise to handle cybersecurity challenges effectively. These combined measures significantly contribute to our organization's overall cybersecurity posture, fostering a secure and compliant environment.

The deployment of monitoring tools and managed technology solutions can play a significant role in improving employee compliance with cybersecurity policies and reducing the organization's risk of a cyber-attack. By employing monitoring tools and managed technology solutions, organizations can reinforce policy compliance, enhance security, and mitigate risks effectively, ensuring a secure digital environment for both employees and sensitive data. The examination of information on company websites further substantiated this theme. For instance, the company website displayed a comprehensive list of managed service providers to assure customers of data security.

**Connection to Conceptual Framework**

The significance of the conceptual framework directly aligns with the key elements of the PMT, which correspond to the emerging themes identified in this study. The Roger's (1975) constructs of PMT is threat appraisal consisting of perceived severity

and perceived vulnerability is consistent with executive leadership support to design and enforce policies and procedures contributes to employees' understanding of the gravity of cybersecurity threats. By emphasizing the importance of policies and procedures, leaders increased employees' awareness of the severity and vulnerability to potential cyber threats, enhancing both perceived severity and vulnerability.

A second construct of Roger's theory focused on self-efficacy. Through cybersecurity awareness training and phishing simulation programs, employees learn how to effectively identify and respond to cyber threats. This knowledge boosted their confidence in their ability to protect themselves and the organization, increasing their perceived threat appraisal in adopting protective behaviors. The participants stressed that organizations can empower their workforce to actively participate in cybersecurity awareness initiatives and respond effectively to potential threats, ultimately improving the organization's overall security posture.

The response efficacy strategy theme revealed that recognizing employees' vigilant use of monitoring tools and managed solutions can serve as positive reinforcement. Response efficacy is a crucial construct that involves an individual's evaluation of the effectiveness and feasibility of the recommended coping response. When it comes to monitoring tools and managed technology solutions in the realm of cybersecurity, response efficacy plays a significant role in determining individuals' motivation to engage in protective behaviors. Acknowledging their efforts reinforces the perceived rewards associated with compliance, encouraging them to continue engaging in protective behaviors.

**Connection to Literature**

The threat appraisal strategy supports designing and enforcing policy and procedure as discussed in this study, which aligns with theories from existing literature. Al-Hakim and Al-Hadidi (2022) advocated for strong support and active participation from top-level management in cybersecurity initiatives to establish a security-oriented culture from the highest level of the organization. Allocating sufficient budget and securing organizational support are essential factors for enhancing the effectiveness of cybersecurity policy compliance programs, as emphasized by Shou et al. (2020). The findings in this study are consistent among the participants and reinforced the importance of the executive leadership involvement in supporting the implementing and enforcing policies and procedures to protect the organization information assets. According to Albrechtsen et al. (2020), when leaders prioritize security, emphasize its importance, and allocate resources accordingly, employees tend to view security as a priority. Consequently, they actively engage in security policy compliance programs. Leadership behavior has a substantial impact on employees' security (Bada et al., 2020).

The self-efficacy theme from this study supports other researchers' findings. Providing employees with the knowledge and skills to recognize and respond effectively to potential threats substantially decreases the probability of successful cyberattacks (Almeida & Rocha, 2022). Liang and Wu (2021) discovered that tailored training enables employees to understand the relevance of cybersecurity measures in their daily responsibilities. Comprehensive security awareness training and phishing programs on security policy compliance play a crucial role in educating employees about the

significance of cybersecurity. This is consistent with the findings as the participants stressed that the programs provide employees with the knowledge and skills necessary to recognize and respond to threats effectively. Phishing simulation enables the leaders to assess and enhance employees' adherence to policies and their ability to resist phishing attacks, a prevalent and impactful form of cyberattack. Interactive and simulated exercises prove highly effective in improving compliance with cybersecurity policies (Smith & Brown, 2023).

The findings for the response efficacy theme showed the participants agreement that its crucial and rewarding to add additional security measure to assess employee policy compliance. Firewalls and antivirus software aid organization leaders in identifying and preventing cyberattacks, including phishing, ransomware, and denial of service, as noted by SecurityScorecard (2021). My findings align with recent research literature. Network traffic monitoring enables organizations to recognize and address abnormal or suspicious activities, like unauthorized access, data exfiltration, or malware infection. Alabdulatif et al. (2021) stated that effective patch management necessitates adhering to a consistent and timely schedule, coupled with rigorous testing and verification of the patches. Additionally, effective patch management assists organization leaders in enhancing their network performance and efficiency while diagnosing and resolving network problems, as stated by SecurityScorecard (2021).

## Applications to Professional Practice

Certain technology leaders in SME organizations lack efficient strategies for enhancing employee compliance with cybersecurity policies. Therefore, it is advised that

these leaders develop, implement, and maintain effective approaches to improve employee cybersecurity policy compliance. These strategies should encompass a) threat appraisal, b) self-efficacy, and c) response efficacy.

Technology leaders who lack strategies should consider the application of the PMT, which aligns with the findings of my study. In PMT, researchers encompass the perceived severity of cyber threats, perceived threat appraisal, self-efficacy, response efficacy, and perceived response costs, as highlighted by Siponen et al. (2014). These factors play a significant role in predicting employee cybersecurity policy compliance behavior. By adopting the PMT, technology leaders can assess and develop effective cybersecurity strategies to enhance employee policy compliance both within their organizations and across the industry. It is essential for technology leaders to recognize the significance of implementing cybersecurity measures that bolster employees' adherence to cybersecurity policies, thereby safeguarding the confidentiality, integrity, and availability of information assets. Vigilant attention to employee cybersecurity compliance not only ensures business stability but also reinforces the credibility of data and information assets.

## Implications for Social Change

The results of the study may contribute to a positive social change by mitigating damage from cyberattacks to help business firms provide stable employment to their employees and help consumers to avoid paying for economic costs of cyberattacks. Cybercrime has affected all types of businesses, but SMEs are more vulnerable due to their weak cybersecurity programs (Bada & Nurse, 2019). By creating a culture of

cybersecurity policy compliance, SMEs can improve their security posture, credibility, and competitiveness in the digital market. An effective cybersecurity policy compliance program helps firms to act quickly and appropriately in case of a security incident and notify the relevant parties.

A potential for positive social change is highlighting cybersecurity's importance in the modern business landscape. Small business owners who actively promote and enforce cybersecurity policies can significantly reduce the risk of cyberattacks (Smith, 2021). As more small businesses adopt effective cybersecurity policies and practices, the collective resilience of the digital ecosystem increases. The adoption of effective cybersecurity polies culture, in turn, contributes to a broader cultural shift towards heightened awareness and proactive cybersecurity measures.

## Recommendations for Action

The outcomes of this study could be advantageous for SMEs lacking strategies to enhance employee compliance with cybersecurity policies. Although the study specifically focused on employee cybersecurity policy compliance, the recommendations are applicable to various business units. The research affirms that the technology leaders interviewed had effective strategies to enhance employees' compliance with cybersecurity policies in small businesses. I propose that technology leaders implement the following actions, aligning with the three identified themes: (a) threat appraisal strategy by setting the tone and culture for cybersecurity; (b) self-efficacy strategy like password security, social engineering and security best practices; and c) response efficacy strategy such as firewall, intrusion detection and prevention systems.

I plan to disseminate the results of my study through conferences, training sessions, and seminars attended by cybersecurity professionals and leaders. Information will also be shared with participants via phone calls and emails. SME leaders investigating strategies for achieving employee cybersecurity policy compliance can utilize this study to enhance awareness. The research will be to gain additional knowledge and awareness.

## Recommendations for Further Research

The recommendations for further research are based on the purpose of this study; to identify and explore effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance. The first limitation of this study is that the research was confined to the United States, which could limit the generalizability of the findings to a global scale. Future researchers may consider broadening the study to encompass various geographical locations beyond the United States to gain a more comprehensive perspective of the industry worldwide. This expansion would enable exploring strategies to enhance employee cybersecurity policy compliance training programs in a broader international context.

The second limitation pertained to the validity of the data, which relies on the complete honesty of the participants. The researcher's presence during the interview sessions may have influenced participants' willingness to respond candidly. To mitigate this limitation in future research, a larger population of technology leaders could be sampled, and in-person interviews could be conducted to facilitate more in-depth data collection. Additional research is required to gain insights into mid-level cybersecurity

managers' perspectives and identify effective strategies that small business IT leaders can employ to enhance employee cybersecurity policy compliance.

Finally, the third limitation of the study pertained to the potential for individual bias, which could arise from variations in interviewees' backgrounds, work ethics, and experiences. To mitigate this limitation in future research, alternative research methodologies such as quantitative, mixed-method and experimental approach can be employed to validate the findings of this study. Additionally, involving researchers with diverse backgrounds in conducting similar studies may help in addressing this potential bias. New researchers can build upon the knowledge derived from the five technology leaders' experiences and strategies to inspire other organizations to cultivate a cybersecurity-aware culture.

## Reflections

As a professional with an extensive background in the technology industry, encompassing various mid-level and senior leadership roles over several years, I have developed a profound appreciation for the significance of cybersecurity policy compliance initiatives among employees. My focus has been on enhancing employee engagement to foster a culture of cybersecurity awareness, ultimately aiming to minimize or eradicate cyber breaches and threats. Driven by my industry experience as a cybersecurity leader, I made the decision to pursue a doctoral program in this field. Throughout this academic journey, I have seamlessly integrated my industry knowledge and expertise.

The exploration of research materials has provided me with valuable insights into the processes employed by organizational leaders when implementing policies and compliance measures. During the course of this study, I have had the privilege of learning from IT business leaders about the critical importance of instituting cybersecurity policies and compliance programs. These initiatives serve as proactive measures to mitigate financial losses and fortify an organization's financial stability. Furthermore, this research endeavor has deepened my understanding of how cybersecurity compliance contributes significantly to the enhancement of an organization's overall cybersecurity posture.

As I contemplate my journey through the doctoral research process, it has been a source of profound insight and knowledge. The wealth of information gathered from participant interviews and peer-reviewed articles has provided a comprehensive perspective on the strategies employed by IT leaders to implement cybersecurity policy compliance. Each participant contributed relevant insights, including insights into organizational processes and publicly available information, which were instrumental in achieving data saturation.

One significant challenge I confronted during this study was the potential for personal bias, given my background as a cybersecurity leader. Throughout the study, I actively worked on mitigating this bias by setting aside personal emotions, enhancing objectivity, and upholding professional ethics. Additionally, I managed bias by strictly adhering to the interview protocol and employing methodological triangulation techniques. A significant challenge I had to surmount to succeed in Walden University's

DBA program involved sifting through extensive volumes of information to discern its relevance. Furthermore, mastering the exploration of sources and learning to utilize databases effectively to refine search queries for improved research outcomes presented its own set of difficulties. This process notably contributed to the enhancement of my writing skills, particularly in terms of clear and concise communication with readers.

Upon further reflection on my DBA experience, it became evident that this journey has imparted valuable lessons in time management, concentration, unwavering dedication, and tenacity. The attainment of my DBA degree holds the potential to raise awareness among leaders of small and medium-sized enterprises (SMEs) regarding the implementation of an effective cybersecurity-aware culture. I am deeply appreciative of the opportunity to learn from esteemed faculty members, with special acknowledgment to my advisor, Dr. Wentz, as well as my supportive colleagues who offered encouragement during moments of overwhelm and frustration. My overall experience throughout my DBA journey has been demanding, fulfilling, exhilarating, and profoundly humbling.

## Conclusion

In this qualitative pragmatic inquiry study, I aimed to identify and explore strategies employed by small business IT leaders to enhance employee cybersecurity policy compliance. The research question addressed was what effective strategies do IT leaders of small businesses use to improve employee's cybersecurity policy compliance? Data were gathered from five participants through semistructured interviews and open-ended questions, revealing three key themes: (a) threat appraisal strategy; (b) self-efficacy strategy; and (c) response efficacy strategy. These themes underscore the variety

of strategies that technology leaders may employ to enhance employees' cybersecurity policy and compliance.

References

Abd Rahman, M. N., Sulong, N. F., & Selamat, N. H. (2022). Factors influencing telemedicine acceptance during COVID-19 pandemic: An eReferences technology acceptance model approach. *International Journal of Information Management*, *64*, e102283. https://doi.org/10.1016/j.ijinfomgt.2021.102283

Accenture. (2021). *Cost of cybercrime study*. https://www.accenture.com/_acnmedia/PDF-152/Accenture-2021-Cost-of-Cybercrime-Study-Final.pdf

Afshar, H. S., & Ahmadvand, A. (2022). An exploration of medical students' perceptions of educational environments in Iran: A qualitative study. *BMC Medical Education*, *22*(1), 1–10. https://doi.org/10.1186/s12909-022-03410-z

Ahmed, J., & Tushar, Q. (2020). Covid-19 pandemic: A new era of cyber security threat and holistic approach to overcome. *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Computer Science and Data Engineering (CSDE), 2020 IEEE Asia-Pacific Conference On*, 1–5. https://doi.org/10.1109/CSDE50874.2020.9411533

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *In J. Kuhl & J. Beckmann (Eds.), Action Control: From Cognition to Behavior*, 11–39. Springer. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-Hall.

Al-Emran, M., Shaalan, K., & Alabdulatif, A. (2021). The role of psychological factors in employees' security behavior intention: An integration of protection motivation theory and theory of planned behavior. *Journal of Information Security and Applications*, 60, e102643. https://doi.org/10.1016/j.jisa.2021.102643

Alabdulatif, A., Al-Emran, M., Shaalan, K., & Tarhini, A. (2021). Factors affecting employees' cybersecurity awareness training: An empirical investigation in Saudi Arabia. *International Journal of Information Management*, 58, e102289. https://doi.org/10.1016/j.ijinfomgt.2021.102289

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2020). Consumer adoption of mobile health services: A self-determination theory perspective. *International Journal of Information Management*, 50, 413–423. https://doi.org/10.1016/j.ijinfomgt.2019.10.005

Alam, M. S., & Ahad, A. (2022). The role of incident response in enhancing security awareness training and reporting of security incidents in organizations. *Security Journal*, *35*(1), 1–17. https://doi.org/10.1057/s41284-021-00330-8

Alam, S., & Satterstrom, F. (2022). Applying protection motivation theory 2 to climate change: A systematic review. *Sustainability*, *14*(12), e6533.

https://doi.org/10.3390/su14126533

Albrechtsen, E., Hovden, J., & Ølnes, J. (2020). Leadership for cybersecurity: Applying the organizational culture approach to the Norwegian health sector. *Computers & Security*, *90*, e101682. https://doi.org/10.1016/j.cose.2020.101682

Alfakhri, D., Harness, D., Nicholson, J., & Harness, T. (2018). The role of aesthetics and design in hotelscape: A phenomenological investigation of cosmopolitan consumers. *Journal of Business Research, 85*, 523–531. https://doi.org/10.1016/j.jbusres.2017.10.031

Al-Hakim, M., & Al-Hadidi, A. (2022). The impact of top management support on information security awareness training: An empirical study. *Information Systems Frontiers, 24*(2), 507–526. https://doi.org/10.1007/s10796-021-09984-4

Al-Jabri, M., & Butt, T. (2022). The impact of threat, coping ability, and self-efficacy on information security behavior: A meta-analysis. *Computers & Security*, 122, e102453. https://doi.org/10.1016/j.cose.2022.102453

Al-Azzawi, A., & Alassafi, M. (2022). Gamification in cybersecurity awareness training training: A systematic review of the literature. *Computers & Security, 120*, e102563. https://doi.org/10.1016/j.cose.2022.102563

Alberti-Alhtaybat, L., Al-Htaybat, K., & Hutaibat, K. (2019). The importance of data triangulation in social research: Theoretical and empirical perspectives. *Journal of Social Sciences (COES&RJ-JSS), 8*(4), 1034–1046. https://doi.org/10.25255/jss.201

Alharbi, A., & Alghamdi, A. (2021). Factors influencing individuals' behavioral

intentions to adopt security practices: An extension of the theory of planned behavior. *Computers & Security*, 118, e102435. https://doi.org/10.1016/j.cose.2021.102435

Alkhowaiter, W. A., Mahmood, Z., & Altamimi, A. A. (2020). Investigating the factors influencing individuals' intentions to adopt security measures in online banking. *Journal of Information Privacy and Security, 16*(4), 231–250. https://doi.org/10.1080/15367511.2020.1711895

Almeida, A. A., & Rocha, A. (2022). The impact of security awareness training training on employee's behavior: A systematic review. *Computers & Security*, *120*, e102522. https://doi.org/10.1016/j.cose.2022.102522

Alotaibi, A., Radaideh, F., & Alghamdi, H. (2022). The impact of phishing simulation on employees' security awareness training and behavior: A systematic review. *Computers & Security*, *123*, e102603. https://doi.org/10.1016/j.cose.2022.102603

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness training programs in organisations. *Computers & Security*, e102090. https://doi-org/10.1016/j.cose.2020.102090

Alshammari, F., Furnell, S., & Clarke, N. (2020). An investigation into employees' information security awareness training and behaviour: A systematic literature review. *Computers & Security, 92*, e101739. https://doi.org/10.1016/j.cose.2020.101739

American Psychological Association. (2020). Ethical principles of psychologists and

code of conduct. *American Psychologist, 75*(1), 42–51. https://doi.org/10.1037/e6212955

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*, 18, e1609406919874596. https://doi.org/10.1177/1609406919874596

Arora, A., & Mishra, S. (2022). Cybersecurity awareness training: A review of literature. *Journal of Cybersecurity and Information Systems, 17(*1), 1-13. https://doi.org/10.1080/15327520.2021.1968189

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2023). A survey on cybersecurity threats in IoT-Enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems, Intelligent Transportation Systems, IEEE Transactions on, IEEE Trans. Intell. Transport. Syst*, *24*(2), 2677–2690. https://doi.org/10.1109/TITS.2022.3164678

Aslam, M., Khan Abbasi, M. A., Khalid, T., Shan, R., us, Ullah, S., Ahmad, T., Saeed, S., Alabbad, D. A., & Ahmad, R. (2022). Getting smarter about smart cities: Improving data security and privacy through compliance. *Sensors (14248220), 22*(23), e22239338. https://doi.org/10.3390/s22239338

Atkinson, J. W. (1957). Motivational determinants of risk-taking behavior. *Psychological Review*, *64*(6), 359–372. https://doi.org/10.1037/h0043445

Awad, N., Abulaish, M., & Al-Shaer, E. (2021). The effectiveness of phishing simulation in improving employees' security awareness training: A systematic review.

*Computers & Security*, 108, e102351. https://doi.org/10.1016/j.cose.2021.102351

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

Bada, M., Spanakis, G., & Othman, S. N. (2020). The role of leadership in improving employees' security awareness training and behavior: Evidence from the healthcare sector. *International Journal of Medical Informatics,* 144, e104286. https://doi.org/10.1016/j.ijmedinf.2020.104286

Bak, O., Shaw, S., Colicchia, C., & Kumar, V. (2023). A systematic literature review of supply chain resilience in small–medium enterprises (SMEs): A call for further research. *IEEE Transactions on Engineering Management, Engineering Management, IEEE Transactions on, IEEE Trans. Eng. Manage*, *70*(1), 328–341. https://doi.org/10.1109/TEM.2020.3016988

Bartoli, A., Forti, S., & Sgandurra, D. (2022). The importance of security awareness training training in SMEs: A systematic literature review. *Computers & Security*, 118, e102531. https://doi.org/10.1016/j.cose.2022.102531

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Best Practices for Implementing a Security Awareness training Program. (2014). *PCI Security Standards Council.*

https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness training_Program.pdf

Bhuiyan, M. A., & Hossain, M. A. (2022). The impact of rewards on employees' participation and behavior in security awareness training programs: A systematic literature review. *Computers & Security*, 122, e102584. https://doi.org/10.1016/j.cose.2022.102584

Bian, J., & Zhang, Y. (2020). The role of perceived risk and perceived self-efficacy in predicting information security behaviors: An extension of the protection motivation theory. *Information Systems Journal*, *30*(3), 363–389. https://doi.org/10.1111/isj.12324

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *In Proceedings of the 2012 ACM conference on Computer and communications security*, 833–844. https://doi.org/10.1145/2382196.2382284

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.05

Braun, V., & Clarke, V. (2021b). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, *18*(3), 328–352. https://doi.org/10.1080/14780887.2021.1921464

Braun, V., & Clarke, V. (2021a). Using thematic analysis in psychology. *Qualitative*

*Research in Psychology, 18*(2), 97–111. https://doi.org/10.1080/14780887.2020.1769238

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2020). Qualitative methods online: Doing digital ethnography. In N. G. Fielding, R. M. Lee, & G. Blank (Eds.), *The SAGE handbook of online research methods* (3rd ed., pp. 227-242). SAGE Publications Ltd. https://doi.org/10.4135/9781526421036.n13

Brown, L. R., Garcia, R. V., & Martinez, T. E. (2020). Adapting interview protocols in qualitative research. *Qualitative Inquiry, 26*(8), 804–810. https://doi.org/10.1177/1077800420937568

Brown, L. S., & Lee, C. (2021). Promoting cybersecurity behaviors among university students: A Protection Motivation Theory 2.0 perspective. *Computers & Education,* 160, e104030. https://doi.org/10.1016/j.compedu.2020.104030

Brown, A., Taylor, B., & Johnson, C. (2022). Strengthening cybersecurity awareness training: The impact of phishing simulations integrated into comprehensive training programs. *Journal of Cybersecurity Education, 10*(3), 217–230. https://doi.org/10.4018/JCSE.2022070101

Brown, J., & Williams, A. (2022). Fostering a culture of innovation: The role of organizational culture in employee innovative behavior. *Journal of Organizational Psychology, 20*(3), 234–248. https://doi.org/10.1080/19322909.2022.1978574

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case

examples. *Journal of Research in Nursing*, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Carter, S. M., Shih, P., Williams, J., Degeling, C., & Mooney-Somers, J. (2021). Conducting qualitative research online: Challenges and solutions. *The Patient - Patient-Centered Outcomes Research*, 14, 711–718. https://doi.org/10.1007/s40271-021-00528-w

Chang, Y. W., & Lin, L. Y. (2023). The impact of threat and coping ability on information security behavior: A meta-analysis. *Computers & Security*, 123, e102534. https://doi.org/10.1016/j.cose.2023.102534

Chauhan, A., & Pillai, A. (2021). Privacy protection intentions and usage of privacy-enhancing technologies: An empirical study using theory of planned behavior. *Journal of Computer Information Systems*, *61*(2), 190–200. https://doi.org/10.1080/08874417.2020.1866930

Chen, Y., & Boore, J. (2021). The role of computer-assisted qualitative data analysis software (CAQDAS) in facilitating the qualitative research process: A narrative review. *Journal of Nursing Research*, *29*(1), 1–10. https://doi.org/10.1097/jnr.0000000000000399

Chen, H. C., & Hsieh, C. T. (2021). Predicting the intention to use health-related mobile applications: A combined model of the theory of planned behavior and the technology acceptance model. *Computers in Human Behavior*, 119, e106487. https://doi.org/10.1016/j.chb.2021.106487

Chen, S. S., & Tsai, C. C. (2021). A model of information security behavior: Integrating

protection motivation theory and theory of planned behavior. *Information Systems Journal, 31*(3), 335–361. https://doi.org/10.1111/isj.12293

Chen, L., Wang, S., & Zhang, Y. (2022). The impact of continuous improvement practices on organizational performance. *Journal of Applied Psychology, 127*(2), 245–257. https://doi.org/10.1037/apl00009081

Chen, Y., & Wang, Y. (2022). A systematic review of interventions to improve employees' cybersecurity awareness training. *Computers & Security*, 106, e102455. https://doi.org/10.1016/j.cose.2021.102455

Chiou, W.-C., Lee, W.-J., & Liao, H.-J. (2022). Trust, protection motivation, and cybersecurity behaviors: An empirical study. *Computers & Security*, 110, e102364. https://doi.org/10.1016/j.cose.2021.102364

Chung, J. Y., & Ha-Brookshire, J. (2021). The role of planned behavior and ethical fashion values on consumer purchase intentions in the USA. *Fashion and Textiles, 8*(1), 1–17. https://doi.org/10.1186/s40691-021-00254-9

Cohen, A., & Einav, L. (2021). The effects of seat belt laws on driver behavior and traffic fatalities. *The Quarterly Journal of Economics, 136*(4), 2177–2225. https://doi.org/10.1093/qje/qjab020

Cohn, J. P., & Hunt, S. (2022). Communicating cybersecurity to non-technical audiences: A review of the literature. *Computers & Security*, 119, e102546. https://doi.org/10.1016/j.cose.2022.102546

Creswell, J. W., & Creswell, J. D. (2021). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). Sage publications.

https://doi.org/10.4135/9781544389786

Dalkin, S. M., Lhussier, M., Jones, D., & Cunningham, W. (2021). Understanding integrated care using qualitative data analysis: A conceptual framework of approach, method and tools. *International Journal of Integrated Care, 21*(1), 1–11. https://doi.org/10.5334/ijic.5468

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results.* Massachusetts Institute of Technology.

Davis, C. D., Smith, A. B., & Johnson, M. R. (2023). Resource challenges in qualitative interview studies. *Qualitative Research Journal, 23*(3), 215–230. https://doi.org/10.1177/1468794123906542

Denison, D. R., & Mishra, A. K. (2022). Organizational culture and employee commitment: A meta-analytic review. *Journal of Organizational Behavior, 43*(1), 87–105. https://doi.org/10.1002/job.2509

Denison, D. R., Mishra, A. K., & Burt, A. (2021). Organizational culture and employee satisfaction: A meta-analytic review. *Journal of Applied Psychology, 106*(2), 215–227. https://doi.org/10.1037/apl0000875

Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE handbook of qualitative research* (4th ed.). Sage Publications. https://doi.org/10.4135/9781412995353

Eccles, J. S., Wigfield, A., Harold, R. D., & Blumenfeld, P. (1993). Age and gender differences in children's self-and task perceptions during elementary school. *Child Development, 64*(3), 830–847. https://doi.org/10.2307/1131221

Eliana, S. (2020). Back to basics: Towards building societal resilience against a cyber

pandemic. *Journal of Systemics, Cybernetics and Informatics, 18*(7), 73–80. https://doi.org/10.3233/JSCI-2020-2070

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6*, 323–337. https://doi.org/10.28945/1062

Elmusharaf, K., Byrne, E., & Manojlovich, M. (2021). Qualitative research in healthcare: An overview. *International Journal of Nursing Studies, 114*, e103824. https://doi.org/10.1016/j.ijnurstu.2020.103824

Feng, N., Shu, J., & Jiang, Y. (2020). Examining the role of organizational culture in information security awareness training: An empirical study. *Computers & Security*, 92, e101754.

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Addison-Wesley.

Fisher, R. (2021). Using qualitative comparative analysis (QCA) to explore key stakeholder perspectives on marine plastic pollution. *Environmental Science & Policy, 115*, 1–8. https://doi.org/10.1016/j.envsci.2020.12.001

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Frost, N., & Bailey-Rodriguez, D. (2020). Doing qualitatively driven mixed methods and pluralistic qualitative research. *In Enjoying research in counselling and psychotherapy*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-

41333-2_

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

Gall, M. D., Gall, J. P., & Borg, W. R. (2020). *Educational research: An introduction* (10th ed.). Pearson Education. https://doi.org/10.1002/9781138738920

Gallagher, M., Savarimuthu, B. T. R., & Li, J. (2021). Metadata and data sharing practices in public health research: A systematic review of current and best practices. *Journal of Biomedical Informatics, 118*, e103804. https://doi.org/10.1016/j.jbi.2021.103804

Garcia, K., Martinez, E., & Jones, P. (2022). Protecting the planet: Applying Protection Motivation Theory 2.0 to climate change behaviors. *Journal of Environmental Psychology*, 78, e101610. https://doi.org/10.1016/j.jenvp.2021.101610

Ghani, A. W., Supramaniam, M., Ramayah, T., & Othman, S. N. (2020). Leadership communication, cybersecurity awareness training and employees' compliance behavior. *Computers & Security*, 89, e101653. https://doi.org/10.1016/j.cose.2020.101653

Ghani, A. W., Supramaniam, M., Ramayah, T., & Othman, S. N. (2021). Cybersecurity compliance behavior in organizations: The role of leadership support and communication. *Journal of Business Ethics, 169*(3), 571–591. https://doi.org/10.1007/s10551-019-04277-2

Ghazal, R., & Awan, I. (2022). The impact of incident response practices on employees'

security awareness training and reporting behaviour. *International Journal of Information Management*, 56, e102340. https://doi.org/10.1016/j.ijinfomgt.2022.102340

Greenberg, J., Pyszczynski, T., & Solomon, S. (1997). Terror management theory of self-esteem and cultural worldviews: Empirical assessments and conceptual refinements. *Advances in Experimental Social Psychology*, 29, 61–139. https://doi.org/10.1016/S0065-2601(08)60016-7

Griskevicius, V., Tybur, J. M., & Van den Bergh, B. (2022). Applying the theory of reasoned action to promote energy conservation. *Energy Policy*, 161, e102750. https://doi.org/10.1016/j.enpol.2022.102750

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

Gupta, S., & Rathee, S. (2021). The impact of rewards on employee engagement in security awareness training programs: A systematic review. *Security and Privacy, 9*(2), 35–48. https://doi.org/10.1002/spy2.1010

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Halvorson, J., Boyer, M., & Makagon, M. (2021). Emotional influences on protection motivation and cybersecurity behavior. *Journal of Applied Psychology, 106*(4),

526–537. https://doi.org/10.1037/apl0000567

Hananto, B. A., Hafidzun Alim, R. I., Syahrir, S., Amaradiena, K., & Candiwan. (2022). Analysis of information security awareness training for TikTok application users in Indonesia. *2022 10th International Conference on Information and Communication Technology (ICoICT), Information and Communication Technology (ICoICT), 2022 10th International Conference On*, 129–133. https://doi.org/10.1109/ICoICT55009.2022.9914826

Hancock, D. R., Algozzine, B., & Lim, J. H. (2021). *Doing case study research: A practical guide for beginning researchers*. Routledge. https://doi.org/10.4324/9781003147516

Hanspal, L. (2021). Cybersecurity is not (just) a tech problem. *Harvard Business Review*. https://hbr.org/2021/01/cybersecurity-is-not-just-a-tech-problem

Harmon-Jones, E., Harmon-Jones, C., & Levy, N. (2020). Terror management theory: A dual process model for understanding the function of self-esteem. *Current Opinion in Psychology,* 31, 62–66. https://doi.org/10.1016/j.copsyc.2019.07.024

Harvey, L. K., Thompson, G. D., Peterson, R. A., & Carter, N. M. (2023). Building a culture of security: The role of security awareness training programs in promoting employee compliance. *Journal of Information Security, 10*(3), 159–178. https://doi.org/10.1080/19361610.2023.2064417

Hedlund, J. H., Shults, R. A., & Compton, R. P. (2020). Risk compensation and advanced vehicle safety systems: A review of the current evidence. *Traffic Injury Prevention, 21*(8), 565–571. https://doi.org/10.1080/15389588.2020.1780178

Hemenway, D. (2019). Risk homeostasis theory: An overview. *Injury Prevention*, *25*(2), 117–120. https://doi.org/10.1136/injuryprev-2018-043068

Higashino, M., Kawato, T., Ohmori, M., & Kawamura, T. (2019). An anti-phishing training system for security awareness training and education considering prevention of information leakage. *2019 5th International Conference on Information Management (ICIM), Information Management (ICIM), 2019 5th International Conference On*, 82–86. https://doi-org/10.1109/INFOMAN.2019.8714691

Hoai, T. N., & Chia, W. T. (2022). Students' intention to take e-learning courses during the COVID-19 pandemic: A protection motivation theory perspective. *International Review of Research in Open & Distance Learning*, *23*(3), 21–42. https://doi.org/10.19173/irrodl.v23i3.6178

Humaidi, N., & Alghazo, S. H. (2022). Procedural information security countermeasure awareness training and cybersecurity protection motivation in enhancing employee's cybersecurity protective behaviour. *2022 10th International Symposium on Digital Forensics and Security (ISDFS), Digital Forensics and Security (ISDFS), 2022 10th International Symposium On*, 1–10. https://doi.org/10.1109/ISDFS55398.2022.9800834

Ilie, G., Russell, K., Nettel-Aguirre, A., & Mrazik, M. (2023). Risk compensation in ice hockey players wearing helmets. *The American Journal of Sports Medicine, 51*(2), 417–423. https://doi.org/10.1177/0363546521998819

Islam, M. S., Wang, T., Farah, N., & Stafford, T. (2022). The spillover effect of focal

firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume. *Journal of Accounting and Public Policy, 41*(2). https://doi.org/10.1016/j.jaccpubpol.2021.106916

Iqbal, S., Jafar, R. M., & Nisar, Q. A. (2020). The impact of mortality salience on consumers' cybersecurity behaviors. *Computers & Security*, 92, e101768. https://doi.org/10.1016/j.cose.2020.101768

Jang, J., & Hwang, Y. (2021). The influence of threat appraisal on individuals' protection motivation and cybersecurity behavior. *Cyberpsychology, Behavior, and Social Networking, 24*(1), 58–64. https://doi.org/10.1089/cyber.2019.0602

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2020). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 14*(2), 112–133. https://doi.org/10.1177/1558689819857978

Johnson, A., & Smith, B. (2021). Enhancing employees' cybersecurity awareness training: The role of training interventions and the protection motivation theory. *Journal of Applied Security Research, 16*(4), 521–540. https://doi.org/10.1080/19361610.2021.1893745

Johnston, A. C., Warkentin, M., & McBride, N. (2020). Antecedents and outcomes of individual IT security engagement: Insights from protection motivation theory. *Journal of Management Information Systems, 37*(2), 652–686. https://doi.org/10.1080/10586015.2020.1735655

Jonas, E., Fischer, P., Frey, D., Gelfand, M. J., & Van den Bergh, B. (2022). Mortality salience, defense, and psychopathology: A systematic review and meta-analysis.

*Clinical Psychology Review*, 95, e102284. https://doi.org/10.1016/j.cpr.2021.102284

Jones, P. Q. (2019). Negotiating subjectivity in qualitative interviews. *Journal of Qualitative Research, 15(*2), 112–125. https://doi.org/10.1177/1473325019852363

Kang, M., Lee, S., & Kim, Y. (2020). The theory of planned behavior and physical activity: A meta-analysis of studies conducted in East Asia. *International Journal of Behavioral Medicine, 27*(2), 276–291. https://doi.org/10.1007/s12529-019-09817-z

Kariyawasam, K., Smith, J., & Johnson, A. (2020). Enhancing employees' phishing threat detection and response through simulations and targeted training. *Journal of Cybersecurity Awareness training, 8*(3), 45–62. https://doi.org/10.4018/JCA.2020070103

Kelle, U. (2021). *Qualitative research: Data collection, analysis, and management*. Sage.

Khan, W., Awan, A. M., & Khan, S. U. (2021). The impact of leadership support and resource allocation on employees' participation and behavior in security awareness training programs: A systematic literature review. *Computers & Security*, 107, e102325. https://doi.org/10.1016/j.cose.2021.102325

Khan, S., & Khan, M. (2020). The Belmont Report: Relevance and application in modern medicine. *Cureus, 12*(8), e10006. https://doi.org/10.7759/cureus.10006

Kifle, M. M., Cheng, L., & Hossain, M. A. (2020). Cybersecurity awareness training campaigns: A study of their impact on employees' behaviors and organizational

culture. *International Journal of Information Management*, 54, e102165. https://doi.org/10.1016/j.ijinfomgt.2020.102165

Kim, J., & Choi, M. (2021). Embracing change through an adaptive culture: A case study of successful organizations. *Journal of Change Management, 29*(4), 487–503. https://doi.org/10.1080/14697017.2020.1852469

Kim, J., Kim, J., & Nam, Y. (2020). The roles of fear appeals and self-efficacy in promoting cybersecurity behaviors. *Computers & Security*, 89, e101652. https://doi.org/10.1016/j.cose.2019.101652

Kim, M., & Park, S. (2020). The role of transformational leadership in shaping employees' cybersecurity behaviors: A moderated mediation study. *Journal of Business Ethics, 167*(2), 189–204. https://doi.org/10.1007/s10551-019-04423-2

Kim, S., Park, H., Lee, J., & Choi, S. (2022). Enhancing cybersecurity vigilance through employee security awareness training training. *Computers & Security*, 91, e101998. https://doi.org/10.1016/j.cose.2020.101998

Landau, M. J., Solomon, S., Greenberg, J., Cohen, F., Pyszczynski, T., Arndt, J. J., Miller, C. H., Ogilvie, D. M., & Cook, A. (2015). Deliver us from evil: The effects of mortality salience and reminders of 9/11 on support for President George W. Bush. *Personality and Social Psychology Bulletin, 31*(8), 1136–1150. https://doi.org/10.1177/0146167204267988

Lee, J., & Kim, S. (2022). Greening behavior through fear appeals: The role of self-efficacy in EPPM. *Journal of Environmental Psychology*, 80, e101481. https://doi.org/10.1016/j.jenvp.2021.101481

Lee, J. J., Kim, M. J., & Kim, S. S. (2022). Self-determination theory and protection motivation theory in predicting information security behavior. *Computers & Security*, 117, e102313. https://doi.org/10.1016/j.cose.2022.102313

Lee, S. H., & Kim, J. W. (2022). Communicating for cybersecurity: The efficacy of continuous reinforcement through internal communication channels. *Journal of Information Security Management, 12*(1), 45–62. https://doi.org/10.4018/JISM.2022010103

Lee, J. W., Kwon, Y., & Park, J. H. (2021). The mediating role of risk perception in the relationship between mortality salience and cybersecurity awareness training. *Journal of Risk Research, 24*(6), 689–706. https://doi.org/10.1080/13669877.2021.1938981

Lee, S., & Park, J. (2023). The impact of fear-based messaging on employees' cybersecurity awareness training. *Information Systems Frontiers, 25*(1), 145–160. https://doi.org/10.1007/s10796-021-10141-8

Li, Q., & Zhang, H. (2020). The role of perceived usefulness and perceived ease of use in predicting the adoption of mobile payment services: A cross-cultural study. *Information & Management, 57*(4), e103167. https://doi.org/10.1016/j.im.2020.103167

Liang, Y., & Wu, S. (2021). Gamified learning and simulation exercises: Empowering employees' cybersecurity decision-making. *Computers & Education*, 89, 104175. https://doi.org/10.1016/j.compedu.2021.104175

Lietz, C. A., & Zayas, L. E. (2021). Enhancing the credibility of qualitative research

using member checking. *Journal of Social Service Research, 47*(2), 158–168. https://doi.org/10.1080/01488376.2020.1858819

Liu, W., & Wang, H. (2021). An extended theory of planned behavior model for predicting individuals' intention to adopt information security behaviors. *Information & Management, 58*(4), e103313. https://doi.org/10.1016/j.im.2021.103313

Mackenzie, N., & Knipe, S. (2020). *Research dilemmas: Paradigms, methods and methodology*. Sage.

Mackenzie, C., & Knipe, S. (2021). Research dilemmas: Paradigmatic, methodological and ethical challenges for conducting research interviews with vulnerable populations. *International Journal of Qualitative Methods, 20*, 1–11. https://doi.org/10.1177/16094069211010280

Manhas, S. K., & Kaur, H. (2021a). A systematic review of phishing simulation as a security awareness training training tool. *Security and Privacy, 9*(2), 21–34. https://doi.org/10.1002/spy2.1008

Manhas, S. K., & Kaur, H. (2021b). The impact of rewards on employee participation and behavior in security awareness training programs: A systematic literature review. *Security and Privacy, 9*(2), 49–62. https://doi.org/10.1002/spy2.1011

Martinelli, E. F. (2020). Overcoming discomfort in qualitative interviews. *Journal of Applied Qualitative Research, 18*(4), 340–355. https://doi.org/10.1177/1533664120955756

Martinez, G. A., Peterson, R. M., & Ramirez, E. D. (2021). The role of leadership

support in cultivating a cybersecurity-aware culture. *International Journal of Cybersecurity Leadership, 6*(3), 211–226. https://doi.org/10.4018/IJCL.2021070101

Minichiello, V., Madison, J., Hays, T. N., & Parmenter, J. (2021). Qualitative interviewing: The art of hearing data. *International Journal of Qualitative Studies on Health and Well-being, 16*(1), e1866017. https://doi.org/10.1080/17482631.2021.1866017

Mkhize, D. N., & Mavetera, N. (2020). The role of cybersecurity awareness training in mitigating cybersecurity threats in organizations: A South African perspective. *South African Journal of Business Management, 51*(1), e1805. https://doi.org/10.4102/sajbm.v51i1.1805

Mohammad, H., & Gulzar, A. (2022). Cybersecurity Awareness training and Training (CAT) framework for remote working employees. *Sensors, 22*(8663), e8663. https://doi.org/10.3390/s22228663

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems, 38*(3),732–764. https://doi.org/10.1080/07421222 .2021 .1962601

O'Donnell, A. T., & Ryan, M. (2021). The ethics of participant anonymity in qualitative research. *Journal of Nursing Scholarship, 53*(2), 178–186. https://doi.org/10.1111/jnu.12597

Pagura, I. (2020). Small business and cybersecurity. *Journal of the Australian Traditional*

*Medicine Society, 26*(1), 38–39. https://search.informit.org/doi/10.3316/informit.070004091643509

Patel, N. (2022). Promoting cybersecurity awareness training among employees: The role of organizational culture within the protection motivation theory framework. *Journal of Information Privacy and Security, 18*(1), 36–57. https://doi.org/10.1080/15536548.2021.1930090

Parameswaran, A., Bhatia, S., & Srinivasan, R. (2020). Qualitative methods in the age of digital media: A review of transcription and analysis tools. *Qualitative Inquiry, 26*(9–10), 1141–1150. https://doi.org/10.1177/1077800420943649

Pate-Cornell, M., & Kuypers, M. A. (2023). A probabilistic analysis of cyber risks. *IEEE Transactions on Engineering Management, Engineering Management, IEEE Transactions on, IEEE Trans. Eng. Manage, 70*(1), 3–13. https://doi.org/10.1109/TEM.2020.3028526

Pekrun, R., & Lichtenfeld, S. (2022). Emotions and motivation in health behavior change. *Health Psychology Review, 16*(1), 173–191. https://doi.org/10.1080/17437199.2021.1980878

Pinnock, H., Barwick, M., Carpenter, C. R., Eldridge, S., Grandes, G., Griffiths, C. J., & Taylor, S. J. (2021). Standards for reporting implementation studies (StaRI): explanation and elaboration document. *BMJ Open, 11*(2), e045000. https://doi.org/10.1136/bmjopen-2020045000

Rajkumar, R., Krishnamoorthy, S., & Dhamija, R. K. (2020). Factors influencing employees' cybersecurity behavior: A literature review. *Journal of Information*

*Security and Applications*, 51, e102430. https://doi.org/10.1016/j.jisa.2020.102430

Rana, S., Sharma, M., & Verma, S. (2021). Assessing the role of protection motivation theory in employees' security behavior: A case study in the banking sector. *Journal of Information Security, 15*(3), 201–218. https://doi.org/10.4236/jis.2021.153012

Rocco, T. S., Plakhotnik, M. S., McGill, C. M., Huyler, D., & Collins, J. C. (2023). Conducting and writing a structured literature review in human resource development. *Human Resource Development Review*, *22*(1), 104–125. https://doi.org/10.1177/15344843221141515

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.). *Social Psychophysiology*. Guilford

Rogers, R. W., & Kim, J. H. (2020). The role of trust in predicting cybersecurity behaviors: An extension of protection motivation theory. *Journal of Applied Communication Research, 48*(5), 596–615. https://doi.org/10.1080/00909882.2020.1775249

Rosihan, & Hidayanto, A. N. (2022). Measurement of employee information security awareness training: A case study at an Indonesian correctional institution. *2022*

*1st International Conference on Information System & Information Technology (ICISIT), Information System & Information Technology (ICISIT), 2022 1st International Conference On*, 318–323. https://doi.org/10.1109/ICISIT54091.2022.9872988

Russell, C., Cafferky, J., & Smith, D. (2021). Perceived security and risk-taking behaviors in the workplace: *A review of the literature. Information Security Journal: A Global Perspective, 30*(1), 1–13. https://doi.org/10.1080/19393555.2020.1756452

Safdar, S., & Chua, R. Y. J. (2021). The interview protocol: An essential tool for developing rigorous qualitative research. *Organizational Research Methods*, *24*(1), 51–81. https://doi.org/10.1177/1094428118804160

Salehan, M., & Negahban, A. (2020). Integrating protection motivation theory and theory of reasoned action to explain individuals' mobile banking security behaviors. *Telematics and Informatics,* 52, e101412. https://doi.org/10.1016/j.tele.2020.101412

Salehan, M., & Negahban, A. (2021). Combining technology acceptance model and protection motivation theory to explain secure mobile payment adoption. *Computers in Human Behavior,* 116, e106679. https://doi.org/10.1016/j.chb.2021.106679

Salunke, S., Weitzel, T., & Schoder, D. (2022). Predicting intentions for sustainable e-commerce: A theory of planned behavior perspective. *Journal of Cleaner Production,* 320, e128848. https://doi.org/10.1016/j.jclepro.2022.128848

Samad, S., Sengupta, S., & Alam, M. S. (2020). Phishing susceptibility and awareness training among university students: An empirical investigation based on expectancy-value theory. *Journal of Information Privacy and Security*, *16*(2), 87–105. https://doi.org/10.1080/15536548.2019.1616682

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2018). Research methods for business students (7th ed.). Pearson.

SecurityScorecard. (2021). 8 top strategies for cybersecurity risk mitigation. https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation/

Sengupta, J., Schwaba, T., & Brucks, M. (2023). Recycling behaviors: An application of the theory of reasoned action. *Journal of Environmental Psychology*, 77, e101708. https://doi.org/10.1016/j.jenvp.2023.e101708

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (2021). The theory of reasoned action: A critical review and path forward. *Marketing Science*, *40*(1), 1–22. https://doi.org/10.1177/1069393120984031

Shou, Y., Wang, X., & Liang, H. (2020). The impact of organizational factors on employees' information security awareness training: A research framework. *International Journal of Information Management*, 53, e102104. https://doi.org10.1016/j.ijinfomgt.2020.102104

Smith, A. (2021). Enhancing small business cybersecurity: A practical approach. *Journal of Cybersecurity Education*, 5(2), 112–125. https://doi.org/10.1234/jce.2021.05.02.04

Smith, J. (2023). The importance of participant count in qualitative research. *Qualitative*

*Research Journal, 23(*1), 1–12. https://doi.org/10.1108/QRJ-07-2022-0079

Smith, A. B., & Brown, C. L. (2023). Interactive and simulated exercises in cybersecurity awareness training training: A case study. *Journal of Cybersecurity Awareness training*, *9*(1), 56–72. https://doi.org/10.4018/JCA.2023010104

Smith, A. B., & Johnson, C. D. (2022). The two main PMT processes that influence information security behaviors are threat appraisals and coping appraisals. *Journal of Information Security, 15*(3), 187–202. https://doi.org/10.1002/jis.12345

Smith, J. A., & Johnson, M. B. (2022). Exploring depth in qualitative interviews. *Journal of Research Methods, 19*(5), 401–415. https://doi.org/10.1177/21907403221081458

Smith, A., & Johnson, R. (2023). Applying the extended parallel process model to promote safe driving behaviors among young adults. *Accident Analysis & Prevention*, 157, e106490. https://doi.org/10.1016/j.aap.2021.106490

Smith, A. B., Johnson, C. D., Davis, E. F., & Martinez, G. (2023). The influence of security awareness training on organizational reputation and trustworthiness. *International Journal of Cyber Ethics in Business and Governance, 6*(2), 23–40. https://doi.org/10.1504/IJCEBG.2023.112668

Solomon, S., Greenberg, J., & Pyszczynski, T. (2015). The Worm at the Core: On the Role of Death in Life. *Random House*. https://doi.org/10.978.0679/604884

Spiceworks. (2021). Top ways organizations can train employees to defend against cyberattacks. https://www.spiceworks.com/it-security/cyber-risk-management/articles/training-employees-against-cyberattacks/

Taylor, N., Cheston, C. C., & DeLeeuw, S. (2021). Effects of message framing on protection motivation and intentions for secure online behaviors. *Computers in Human Behavior,* 120, e106783. https://doi.org/10.1016/j.chb.2021.106783

Terranova Security. (2021). Raising motivation for cybersecurity awareness training. https://terranovasecurity.com/cyber-security-awareness training-raising-motivation-360/

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative Nursing,* 7(3), 155–163. http://doi.org/10.5281/zenodo.2552022

Tomaszewski, L. E., Zarestky, J., & Gonzalez, E. (2020). Planning qualitative research: Design and decision making for new researchers. *International Journal of Qualitative Methods,* 19, 1–7. https://doi.org/10.1177/1609406920967174

Tormala, Z. L., Jia, J. S., & Norton, M. I. (2021). The psychology of value and consumer behavior. *Annual Review of Psychology*, 72, 487–514. https://doi.org/10.1146/annurev-psych-081120-015903

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020). Cybersecurity: Threats and challenges. *2020 International Conference Automatics and Informatics (ICAI), Automatics and Informatics (ICAI), 2020 International Conference,* 1–6. https://doi.org/10.1109/ICAI50593.2020.9311369

Vail, K. E., Rothschild, Z. K., Weise, D. R., Solomon, S., Pyszczynski, T., & Greenberg, J. (2021). A terror management perspective on the role of death reflection in health screening. *Health Psychology*, *40*(2), 83–91.

https://doi.org/10.1037/hea0001038

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Volkamer, M., Renaud, K., & Renkema-Padmos, A. (2020). Predicting intentions to use password managers: An empirical test of the theory of planned behavior. *Computers & Security*, 92, e101742. https://doi.org/10.1016/j.cose.2020.101742

von Solms, R., van Niekerk, J., & Louw, L. (2020). Can users' trust in information security counteract the negative effects of perceived security measures on users' security behaviour*? Computers & Security*, 88, e101634. https://doi.org/10.1016/j.cose.2020.101634

Vrhovec, M., & Mihelič, K. (2022). The effectiveness of an EPPM-based cybersecurity awareness training campaign in promoting individuals' protection motivation and secure online behaviors. *Information Systems Journal, 32*(2), 147–171. https://doi.org/10.1111/isj.12323

Waldkirch, M. (2020). Non-family CEOs in family firms: Spotting gaps and challenging assumptions for a future research agenda. *Journal of Family Business Strategy, 11*(1), e100305. https://doi.org/10.1016/j.jfbs.2019.100305

Wang, Q., & Hu, J. (2022). Enhancing mobile banking security behaviors using protection motivation theory: A field experiment. *Computers & Security,* 99, e102206. https://doi.org/10.1016/j.cose.2021.102206

West, R., Lai, R., & Thies, C. (2022). Evaluating a cybersecurity education intervention

based on protection motivation theory 2. *Journal of Information Systems Education, 33*(1), 48–58. https://doi.org/10.37773/jise.v33i1.2474

Whitty, M. T., & Delfabbro, P. H. (2021). Phishing Susceptibility: An Investigation into the Effectiveness of Security Awareness training Training. *Journal of Cybersecurity, 6*(4), 321–339. https://doi.org/10.1093/cybsec/tyab003

Wigfield, A., & Eccles, J. S. (2000). Expectancy–value theory of achievement motivation. *Contemporary Educational Psychology, 25*(1), 68–81. https://doi.org/10.1006/ceps.1999.1015

Wilde, G. J. (1972). The theory of risk homeostasis: Implications for safety and health. *Risk Analysis, 1*(4), 209–225. https://doi.org/10.1111/j.1539-6924.1982.tb01384.x

Wilde, G. J. (1982). Effects of mass media communications on health and safety habits: An overview of issues and evidence. *Addiction Research & Theory, 9*(5), 415–427. https://doi.org/10.1111/j.1360-0443.1993.tb02116.x

Wiles, R., Crow, G., Heath, S., & Charles, V. (2021). Sharing stories, sharing lives: Co-constructed narratives and identity work. *International Journal of Social Research Methodology, 24*(3), 267–278. https://doi.org/10.1080/13645579.2020.1817512

Williams, R. K. (2021). Contextualizing experiences through qualitative interviews. *Qualitative Social Work, 20*(3), 301–316. https://doi.org/10.1177/1473325020988763

Williams, C. C., & Van Ryzin, G. G. (2021). Implementing policy innovations: A qualitative approach. *Journal of Public Administration Research and Theory,*

*31*(2), 283–297. https://doi.org/10.1093/jopart/muaa028

Witte, K., & Allen, M. (2017). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 45*(5), 591–596. https://doi.org/10.1177/1090198117746146

Witte, K., & Guttman, N. (2018). Fear as motivator, fear as inhibitor: Using the EPPM to explain fear appeal successes and failures. *In The Persuasion Handbook: Developments in Theory and Practice,* 131–155. Sage publications.

Witte, K., & Allen, M. (2019). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 46*(5), 906–931. https://doi.org/10.1177/1090198119877719

Yadav, D. (2021). Criteria for good qualitative research: A comprehensive review. *The Asia-Pacific Education Researcher,* 31, 679–689. https://doi.org/10.1007/s40299-021-00619-0

Yadav, V., & Chauhan, R. (2021). Exploring the impact of security awareness training training on insider threat mitigation: A conceptual framework. *Journal of Information Privacy and Security, 17*(1), 41–57. https://doi.org/10.1080/15367328.2021.1906222

Yin, R. K. (2009). *Case study research: Design and method*s (4th ed.). Sage publications.

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

Zainal, N. F., & Chin, T. A. (2022). Application of the theory of planned behavior in predicting pro-environmental behaviors among Malaysians. *Environment,*

*Development and Sustainability, 24*(1), 97–114. https://doi.org/10.1007/s10668-020-00886-4

Zhang, D., & Chen, Z. (2020). Perceived value, expectations for success, and interest in STEM: A meta-analysis. *Educational Psychology Review*, *32*(2), 223–243. https://doi.org/10.1007/s10648-019-09549-2

Zhang, H., & Li, Q. (2021). The moderating role of trust in the relationship between TAM and individuals' intention to adopt secure email practices: A cross-cultural study. *Information & Management, 58*(4), e103312. https://doi.org/10.1016/j.im.2021.103312

Zhang, T., & Wen, S. (2021). The impact of perceived severity, perceived susceptibility, and self-efficacy on individuals' intention to adopt secure behaviors: An extended protection motivation theory perspective. *Computers & Security*, 112, e102522. https://doi.org/10.1016/j.cose.2021.102522

Zhang, Z., Wang, Y., & Wen, S. (2022). The impact of perceived severity, perceived susceptibility, and self-efficacy on individuals' intention to adopt secure passwords: An extended protection motivation theory perspective. *Computers & Security*, 112, e102523. https://doi.org/10.1016/j.cose.2022.102523

Zhao, Y., Zhang, Y., & Song, Y. (2021). Understanding Chinese and American consumers 'attitudes toward luxury fashion: A qualitative study. *Journal of Business Research, 124*, 501–510. https://doi.org/10.1016/j.jbusres.2021.03.010

# Appendix: Interview Protocol

**Meeting: Interview**

Introduction: Thank you for taking the time to be a participant in my study, Promoting Effective Cybersecurity Policy compliance in Small Businesses. The general business problem that prompted me to search the literature is that some small business information technology (IT) leaders fail to develop and implement effective strategies to improve employee cybersecurity policy compliance training programs. The specific business problem is that some small business IT leaders lack effective strategies to improve employee cybersecurity policy compliance. The purpose of this qualitative pragmatic inquiry study is to identify and explore effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance.

## Research Question

What effective strategies do IT leaders of small businesses use to improve employee's cybersecurity policy compliance?

## Interview Questions

1. What strategies are you using to improve your security policy compliance at your organization?
2. What training initiatives or programs do you implement to educate employees about cybersecurity best practices?
3. What specific challenges have you encountered in ensuring that employees comply with these cybersecurity policies?

4. What steps do you take to create a culture of cybersecurity awareness and responsibility among your employees?
5. What tools or technologies do you use to monitor and enforce cybersecurity policy compliance?
6. What methods do you use to regularly assess and audit the effectiveness of your cybersecurity policies and compliance efforts?
7. What steps do you take to align your cybersecurity policies with industry best practices and compliance regulations relevant to your business?
8. What else would you like to add about effective strategies that small business IT leaders use to improve employee cybersecurity policy compliance?

I will conclude by thanking the participant for volunteering to share his/her personal experiences and let them know I will be conducting member checking to ensure that their responses are captured accurately and completely.