

11-25-2025

Organizational Leaders' Effective Strategies for Using Employee Training to Mitigate Threats to Cybersecurity Compliance

Oluwaseye Adekunle Fadare
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Oluwaseye Adekunle Fadare

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. Franz Gottlieb, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Yvonne Doll, Committee Member, Doctor of Business Administration Faculty

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

Walden University
2025

Abstract

Organizational Leaders' Effective Strategies for Using Employee Training to Mitigate

Threats to Cybersecurity Compliance

by

Oluwaseye Adekunle Fadare

MSc, Greenwich University, 2008

BSc, Olabisi Onabanjo University, 2003

Research Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2025

Abstract

Organizational leaders increasingly face challenges associated with employee noncompliance with cybersecurity controls, which expose business leaders to reputational and financial risks. Addressing this business problem is critical for cybersecurity leaders and business executives who aim to strengthen digital resilience and sustain profitability. The purpose of this qualitative pragmatic inquiry was to explore effective strategies organizational leaders use to enhance employee cybersecurity compliance through training. The project was grounded in the protection motivation theory and total quality management frameworks, which provide insight into the behavioral and continuous improvement dimensions of cybersecurity management. Six cybersecurity leaders from Nigeria participated in semistructured interviews. Data were analyzed using Braun and Clarke's six-step thematic analysis. Eight key themes emerged: leadership involvement, training effectiveness, customized training strategies, human factors, key cybersecurity threats, awareness programs, compliance challenges, and return on investment. A key recommendation is that business leaders integrate regular updates through tailored and role-specific cybersecurity training to support employees' protection against cyber-threats. The implications for positive social change include the potential to foster a culture of cybersecurity awareness and ethical leadership that protects business and community data, reduces economic losses, and enhances trust in digital environments.

Organizational Leaders' Effective Strategies for Using Employee Training to Mitigate

Threats to Cybersecurity Compliance

by

Oluwaseye Adekunle Fadare

MSc, Greenwich University, 2008

BSc, Olabisi Onabanjo University, 2003

Research Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2025

Dedication

I want to dedicate this project to God for sparing my life to see the completion of this study. I also want to appreciate my loved ones starting with my wife, Foluso, for all the support throughout the journey and my children, Oluwafeyikemi and Abimbola. I also want to thank my brother, Dr. Oluwaseun Fadare, for all the support and encouragement towards the completion of this study. I am also most grateful to my parents and my junior ones, and most especially to Pastor Ebenezer Omotayo, for all the love and prayers.

Acknowledgments

I would like to thank most especially my chair, Dr. Irene Williams, who stood by me throughout this project, for her guidance and mentorship advice. I would also like to thank my second committee member, Dr. Yvonne Doll, for her feedback and advice throughout this project. I also want to appreciate Dr. Franz Michael Gottlieb for his mentorship and contributions towards this project.

I also want to especially thank all my former colleagues at State Street International Ltd. Ireland for all the hard knocks that kept me going to reach the finish line. Even though I almost gave up, God gave me the strength, and the people around me gave me the encouragement and support to keep pushing forward until the goal was achieved. And finally I want to thank all my friends who stood by me and encouraged me all through this program in words and prayers.

To God is all the glory.

Table of Contents

List of Tables	iv
Section 1: Foundation of the Project.....	1
Background of the Problem	1
Business Problem Focus and Project Purpose	1
Research Question	3
Assumptions and Limitations	3
Assumptions.....	3
Limitations	3
Transition	3
Section 2: The Literature Review	5
A Review of the Professional and Academic Literature.....	5
Conceptual Framework.....	7
Protection Motivation Theory.....	10
Cybersecurity Training	13
Insider Threats to, and Cyberattacks on, Organizations	14
Cybersecurity Compliance in Organizations	19
Strategies in Employee Training for Militating Against Cyberattacks and Threats.....	21
Creation of an Organizational Data Handling Policy	25
Emphasis on Employee Training and Responsibility	27
Monitoring and Management of Anomalous Behavior	28

Research Gap	29
Conclusion	29
Transition	30
Section 3: Research Project Methodology	32
Project Ethics	32
Nature of the Project	33
Population, Sampling, and Participants	34
Data Collection Activities	36
Interview Questions	37
Data Organization and Analysis Techniques	38
Reliability and Validity	40
Reliability	40
Validity	40
Transition and Summary	42
Section 4: Findings and Conclusions	43
Presentation of the Findings	43
Theme 1: Leadership Involvement	46
Theme 2: Training Effectiveness, Methods, and Challenges	47
Theme 3: Customized Training Strategies, Continuous Improvement, and Expected Collaboration	49
Theme 4: Human Factor in Cybersecurity and Emerging Technologies	50
Theme 5: Key Cybersecurity Threats	51

Theme 6: Cybersecurity Awareness Strategies.....	52
Theme 7: Compliance and Regulatory Challenges.....	53
Theme 8: Return on Investment on Training.....	54
Connection of the Findings to the Literature Review.....	55
Connection of the Findings to the Conceptual Framework	58
Business Contributions and Recommendations for Professional Practice	65
Implications for Social Change.....	67
Recommendations for Further Research.....	68
Possibilities for Addressing Research Limitations	70
Conclusion	71
References.....	74
Appendix A: Interview Protocol.....	92
Appendix B: Interview Questions.....	93

List of Tables

Table 1. Sources Cited in the Literature Review 6

Table 2. Sources Cited Throughout the Narrative 6

Table 3. Thematic Matrix: Cybersecurity Compliance and Training Strategies 63

Section 1: Foundation of the Project

Background of the Problem

Many business leaders today face exposure to the internet, which has disrupted business activities and resulted in significant financial losses. The emergence of the internet and its benefit has caused an increase in business activities and global exploration of business opportunities. The explosion of business activities online has also resulted in the exposure of businesses to fraudsters and impostors who have deliberately caused harm to the business operations through cyberattacks on businesses (Dearden et al., 2023). Security breaches perpetrated by malicious cyberactors, which have resulted in negative consequences such as loss of confidential data, have led to increased interest in human factors related to security breach incidents and other mitigation approaches (Hughes-Lartey et al., 2021). Due to internet attacks, it is important for business leaders to consider how to safeguard their online activities from both internal and external parties who intend to cause harm to business operations (Saxena et al., 2020). Hughes-Lartey et al. (2021) suggested that to meet system security expectations, business leaders need to consider their employees' behavioral patterns and other human factors. In this project, I explored the threats facing business enterprises online and discussed strategies that can be used to reduce the negative impact and ensure cybersecurity compliance.

Business Problem Focus and Project Purpose

The specific business problem is that some cybersecurity leaders lack effective strategies to improve employee cybersecurity compliance to increase business profitability. Therefore, the purpose of this qualitative pragmatic inquiry project is to

identify and explore some cybersecurity leaders' effective strategies to improve employee cybersecurity compliance to increase business profitability. The project results may help business leaders and senior cybersecurity professionals improve cyberactivities by business enterprises and give more knowledge to business leaders on ways of reducing losses due to cyberattacks. To conduct a viable project, it was necessary to ensure that the sample population was adequate and knowledgeable.

The targeted population consisted of business leaders and security compliance officers of organizations with high online impact in their business activities. I used purposive sampling to identify six participants from my professional and business networks. Eligible participants were business leaders or cybersecurity professionals with supervisory responsibilities in their respective organizations. The research participants were based in Nigeria and were accessed through professional networks. Exclusion criteria eliminated individuals without leadership roles in cybersecurity and with fewer years of experience. The data collection involved the use of semistructured interview questions and publicly available documents. The conceptual frameworks for this project were the protection motivation theory (PMT) and total quality management (TQM).

R. W. Rogers first published the PMT in 1975 to understand how individuals make decisions based on fear and how they protect themselves from negative actions or perceived threats. According to Rogers, an individual's behavior is based on the likely impact of a threat and how best they can protect themselves from such a threat. TQM, on the other hand, is a philosophy developed for management to focus on continuous improvement, customer satisfaction, and employee involvement to achieve business

objectives. The TQM theory, which emerged around the 1980s, was developed by numerous theorists, among who are Edward Deming, Joseph Juran, and Philip Crosby.

Research Question

What effective strategies do some cybersecurity leaders use to improve employee cybersecurity compliance to increase business profitability?

Assumptions and Limitations

Assumptions

Assumptions are facts considered to be true but are not verified (Braun & Clark, 2023). Assumptions carry risk as the basis of the verification may not reflect the true position at the end. Assumptions will help to guide an argument for justification. I assumed that the participants would be willing to participate in the interview and give their honest understanding of the interview questions without any bias.

Limitations

Limitations refer to threats to internal, external, construct, and statistical conclusion validity (Clarke et al., 2023). The limitations of my research project were the need to convince the participants to participate in the project, and the benefits of the project may reduce risks in the cyberworld. Another limitation was ensuring a minimum of six qualified respondents participate.

Transition

In Section 1, I identified the business problem, which is some organizational cybersecurity leaders' lack of strategies to mitigate threats to cybersecurity compliance to increase business profitability. In Section 1, I provided the background for the problem,

addressed the specific business problem, and stated the purpose of the project. I then discussed the assumptions and limitations of the proposed project. In Section 2, I reviewed the professional and academic literature for a wide coverage of the business topic. In Section 3, I discussed project ethics, nature of the project, data collection and analysis methods, and reliability and validity. In Section 4, I discussed the findings and implications for business practice, social change, and further research.

Section 2: The Literature Review

A Review of the Professional and Academic Literature

In this qualitative pragmatic project, I identified the threats of non-compliance with cybersecurity controls on the business enterprise from cybersecurity leaders. I also discussed the various strategies used by managers in preventing and combating insider threats around cybersecurity. In Section 2, I discuss the conceptual framework and the analysis of the two theories that support the research project. Second, I discuss the insider threats and the impact of cyberattack activities in the business environment. Third, I address cybersecurity compliance activities and how business leaders protect their organizations against attacks. Fourth, I discuss employee training and responsibilities as a tool for mitigating against cyberattacks and threats to organizations. Fifth, I discuss how the creation of a data handling policy can help reduce the threats and cyberattacks to an organization. Finally, I discuss the need for and importance of human behavior to monitor and effectively manage security actions to ensure adequate security compliance.

The approach to my literature review involved developing a search using the following keywords: *cybersecurity*, *compliance*, *protection motivation theory*, *information security*, *internal controls*, *systems protection*, *employee management*, *risk*, and *training*. I focused on getting source information that is peer-reviewed and searched through publications between 2020 and 2025. I used the Business Source Complete Databases, which include Science Direct, Open Access Journals, International Security & Counter Terrorism Reference Center, SocINDEX, and ProQuest databases, to access and identify journal articles in the Walden University library databases. Due to the nature of

the business topic, my search strategy initially located articles in cybersecurity compliance within the past 4 years that were peer-reviewed. Due to the inadequate resources from the search, I had to increase the period and the search information to include training, server security threats, and information technology. My search also involved using Google to get some clarity on definitions for adequate use in my project.

The references were verified using Ulrich's periodicals directory to ascertain that the references were peer-reviewed. The total number of references for the literature review was 84 articles. Out of the 85 articles, 69 articles (71.76%) were published in peer-reviewed journals. Out of the articles, 90.59% were published within 5 years of my anticipated graduation date. Table 1 contains a summary of the literature review sources.

Table 1

Sources Cited in the Literature Review

Source	Total no.	No. < 5 years old	% < 5 years old
Peer-reviewed journal article	69	61	71.76
Non-peer-reviewed journal article	3	3	3.53
Book	6	6	7.06
Other	7	7	8.24
Total	85	77	90.59

Table 2 contains a summary of all sources cited in the narrative.

Table 2

Sources Cited Throughout the Narrative

Source	Total no.	No. < 5 years old	% < 5 years old
Peer-reviewed journal article	91	80	74.07
Non-peer-reviewed journal article	3	3	2.78
Book	7	6	5.56

Other	7	7	6.48
Total	108	96	88.89

Conceptual Framework

The PMT and the concept of TQM served as the conceptual framework for this project. The PMT, which Rogers created in 1975, tries to identify the reason why employees fail to adhere to controls established by management against cyberattacks and what can be done to give a positive behavior pattern that will keep them from hurting the business activities (Mou et al., 2022). The TQM originated in the mid-1980s through different prominent theorists, including W Edwards Deming, Joseph Juran, and Philip Crosby. The TQM theory considers the need for continual training and identifying ways to improve the business processes focusing on the interest of the customers and how the business leaders can use the TQM apply training for employees to ensure they stay connected to understand how to improve customer experience at all times. The PMT and TQM theories relates to my research problem of identifying strategies that can help the to improve employee cybersecurity awareness and compliance the PMT and the TQM offer construct that can help business leaders to increase business profitability and reduce negative impact on the operations of the business activities that may be caused by server attacks and exposures of business activities to online networks and applications.

Cybergrowth can offer opportunities to business leaders if properly managed. The increase in cyberactivities over the years has grown to the extent of expanding business activities (Williams et al., 2019). This transition can result in the growth or the extinction of business activities if not adequately monitored and managed by top management

(Pandey et al., 2020; Williams et al., 2019). Increased cyberactivity has resulted in new cybersecurity vulnerabilities to many organizations, such as ransom ware, phishing, zero-day exploits, hacking attempts, and data security risks (Chapman, 2020; Loi & Christen, 2020). These breaches, which may compromise confidentiality or security procedures and policies, may impact an organization's competitive advantage, reputation, and market value (Shaikh & Siponen, 2023). The growth of a business organization due to increased cyberactivities can also result in serious security vulnerabilities that can threaten the business's sustainability if not properly managed.

Cybersecurity also considers human involvement. Organizational leaders can empower their employees to uphold and implement strong security controls. When a company's customers lose trust in the organization because of a security lapse, it could result in lost future earnings, a bad reputation, and litigation against the organization (Alawag et al., 2023; Hubbard et al., 2021; H. Khan & Sukhotu, 2020). Businesses that depend on their customers have historically benefited from the emphasis on raising customer satisfaction, generating better products, and strengthening internal performance (Fornell et al., 2020). Shaikh and Siponen (2023) suggested that due to security lapses or cybersecurity breaches, an organization may face economic consequences such as customer compensation and redressal, cost of lost business, regulatory fines, litigation, regulatory notification, and loss of investments or market value. An organization's financial ruin can result from a loss of public trust, given the amount of media attention that insider threat occurrences receive in today's security-conscious environment (Shaikh & Siponen, 2023). Thus, it is vital to utilize adequate controls to ensure the security of an

organization's data and assets (Chapman, 2020). Human factors and employee behavior are a vital component of enhancing information security in organizations (Hughes-Lartey et al., 2021). Controls should be implemented and managed properly to achieve the desired result. Thus, the responsibility of implementing the controls is vested in the organization's employees.

A unified workforce plays an important role in safeguarding an organization's assets and reputation by promptly addressing its cybersecurity issues. Employee unity in preventing harm to the company's reputation is an essential aspect of adopting an insider threat strategy (Soltani & Wilkinson, 2020). Several studies have reported that employees are important assets in combating cybersecurity-related threats or risks (Alshaikh & Adamson, 2021; Chen et al., 2021; Reeves et al., 2020; Wong et al., 2022). Thus, equipping employees with the right competencies in organizations enables them to better respond to and anticipate potential security threats (Wong et al., 2022). Therefore, organizations should adopt a top-down approach to cybersecurity management (Shaikh & Siponen, 2023). Stakeholder readiness to evaluate their shortcomings to strengthen the organization typically indicates limitations in PMT adoption (Haag et al., 2021). Despite the shortcomings of PMT, there are many benefits to its implementation in safeguarding businesses from security threats.

PMT can be applied to understand and influence employee behavior in a cybersecurity environment. Haag et al. (2021) suggested that PMT is a commonly adopted approach in examining information security behaviors. A well-implemented PMT framework will affect the behavioral outcome of individuals by inducing the fear of

the impact of their actions before they take them (Rogers, 1975). According to Bekkers et al. (2023), the PMT framework is extensively employed to comprehend how people react to stimuli that make them perceive a possible danger. Fear messages that advise people to take precautions or abstain from actions that could endanger themselves or others are among these triggers (McDowell, 2023). Another theory that can help to explore the behavior of employees to cyberattack and control implementation is the TQM. PMT influences behavior through fear, but when applied correctly, it can encourage precautionary actions against cyberattack.

TQM, on the other hand, encourages employees to become stakeholders in the defence process against cyberattack. TQM is a system that helps organizations focus on continual improvement of both products and services by removing any potential obstacles or loopholes that can affect business activities and transactions (Alawag et al., 2023). Streamlining procedures is essential for highly effective teamwork in IT security settings (Reeves et al., 2021). According to Abimbola et al. (2020), every level of the organizational hierarchy can support the advancement of one another by adopting the fundamental TQM values of leadership commitment, continuous improvement, employee education and training, and customer satisfaction. TQM ensures continuous improvement and systematic cohesion by building a cybersecurity culture, team collaboration, and hierarchical empowerment among employees.

Protection Motivation Theory

PMT considers the behavioral pattern and actions that an individual will take towards an expected occurrence or action (Haag et al., 2021). The intention of the need

for an action is a very important factor that drives the behavior of an individual (Haag et al., 2021). According to Rogers (1975), PMT can be used to explain behaviors in response to a threat. This implies that the fear of the outcome of an action will affect and relate to how a person behaves in anticipation of a reasonable action or result. The consideration of not expecting a negative result will therefore enable the individual to take early action to avoid the negativity. The action will be driven by the risk perception and likely result, and the exposures to the organization.

Identifying the reason for protection and the implications of the impact on exposure to risk is very important to any business organization. According to Zuwita and Rahmatullah (2021), the basic notion of PMT is to enable individuals to take adaptive actions in response to risks by perceiving risk vulnerability and considering the options available to remedy these risks through self-efficacy and response efficacy. In appraising threats, the user decides whether they perceive vulnerability to a specific threat and the threat's severity (Zuwita & Rahmatullah, 2021). In coping appraisal, the user determines whether protective actions offer sufficient protection from the threat, the perceived cost of taking protective action, and whether the user can perform the action (Rogers, 1975; Zuwita & Rahmatullah, 2021). Under the PMT model, increased threat vulnerability, threat severity, self-efficacy, and response efficacy aid adaptive behaviors and intentions (Downing et al., 2023). Conversely, adaptive response costs and decreased maladaptive response rewards increase adaptive behavior or intentions (Downing et al., 2023). This indicates that PMT components are beneficial when used for individual and community interventions (Zuwita & Rahmatullah, 2021). Another area to consider is the ability of the

employees to cope with the threats by displaying behaviors that can help to avoid or reduce exposures.

Business leaders and cybersecurity professionals need to recognize threats and understand how to mitigate them effectively. The coping process under the PMT is based on two major fundamentals of appraisal (Downing et al., 2023). The first one is the efficacy of the communicated response, and the second is the self-efficacy of the individual (Downing et al., 2023). This means that efficacy is important and needs to be looked at from the perspective of both the response and the individual responder (Zuwita & Rahmatullah, 2021). The focus of this project will be to consider how effective, accurate, and correct the response or the behavior that initiates the response (Downing et al., 2023). Secondly it will also seek to address how effective the individual's ability or skill to respond accurately to the threat and be able to mitigate it (Downing et al., 2023). Thus, the individual's ability to recognize the threat, know what to do to avoid it or reduce it, and have adequate skills ability for implementation will trigger a coping behavior that protects against identified threats (Liu et al., 2022). The development of an effective coping process skill will help to implement protective behaviors when using online presence to attract more customers.

Business leaders should consider developing policies to identify and mitigate security risks that may affect the organization. The growth of cyberactivities and the dependence of business activities on the internet require businesses to consider actions to protect their resources within and outside the organization (Saxena et al., 2020). Many business leaders have failed because of the inability of their management team to

consider how their business can be impacted by unprotected systems or networks (Saxena et al., 2020). These exposures have made their activities vulnerable and resulted in losses and other negative consequences (Chen et al., 2021). Businesses should therefore consider developing policies that will help to identify and mitigate security risks and increase resilience (Hasan et al., 2021). The purpose of these policies will be to ensure that adequate protection is given to all the various classes of assets being held by the organization (Hasan et al., 2021). Organizational leaders should develop comprehensive policies that protect assets, reinforce resilience, and avoid mistakes due to negligence.

Cybersecurity Training

In addition to the establishment of policies to prevent and protect the organization's assets, cybersecurity training should also be considered by top management as a means of reducing the business's exposure to threats and risks. Training of employees should be a vital activity that should be developed and implemented by top management of organizations (Williams et al., 2019). For training to be effective, businesses must consider the motive of the attacks and how they can prevent those (Williams et al., 2019). In perceiving the threat, the organization identifies a likelihood of the threat first (Williams et al., 2019). Once the likelihood has been ascertained and identified, the secondary stage is initiated, which is based on the threat (Williams et al., 2019). The secondary stage involves the development of activities that will affect the response to the threat (Saxena et al., 2020). This response will involve the appraisal and the coping process (Marina et al., 2023). According to Moody et al. (2018), the individual appraises and determines that he or she can cope with the perceived threat. Once this has

been ascertained, the coping process is initiated, and this helps to identify what needs to be done to reduce the impact of the threat or the behavior that needs to be displayed to overcome the threats (Marina et al., 2020). Identifying the source of the threats can also be beneficial for organizational leaders to implement the best control practices in the organization.

Insider Threats to, and Cyberattacks on, Organizations

Cyberattacks on organizations can come from both internal and external sources. Insider threats are now recognized as one of the many hazards that need to be closely considered. According to a security survey, security incidents are caused mainly by present personnel and then by previous employees (Chen et al., 2021; Khando et al., 2021). Security incidents can also be caused by those who have access to transactions and business activities within the organization (Chapman, 2020). A security survey by Clifton (2024) found that internal threats pose a serious threat. According to the survey, 52% of respondents find it more challenging to handle internal threats than external intrusions, and 68% of firms feel exposed to insider attacks (Clifton, 2024). Less than half of the firms, it is reported, are not sufficiently ready to safeguard their information assets against the potential threats of insider assaults (Clifton, 2024). The result has caused a greater need to focus and concentrate on the activities of employees towards protecting the business.

Perceived personal gains can drive insider threats, and organizations must strategically address both workplace conditions and individual cost-benefit perceptions to minimize risks. Insiders were most likely to divulge private company information in

exchange for financial gain, per the (Fu et al., 2020) insider danger spotlight study. In a similar vein, insiders may be persuaded to act against companies anytime they witness injustice occurring there (Shapira, 2022). Employers have looked for strategies to lessen emotional strain and meet workers' needs to decrease workers' discontent with their companies and workplaces, considering these findings (H. Lee, 2021). This strategy, though, has come under fire for having fundamental flaws in its comprehension of human nature (Ray et al., 2020). Individuals choose to commit crimes because of differences in the costs and benefits, not because their reasons are different from others (Ray et al., 2020). The intention to commit a crime is also examined when the potential benefit of the crime outweighs the cost to the individual or perpetrator. The benefit can be financial or otherwise, as much as it motivates the action to commit the crime (Ray et al., 2020). This assertion aligns with the rational choice theory, which suggests that malevolent insiders will only engage in illicit activities if the benefits of their malicious actions are above the projected dangers or expenses (Alawag et al., 2023). It is important to assign security maintenance and protection responsibilities to experts and professionals.

Business leaders and compliance officers should implement strategic controls that balance security measures with employee responsibilities to maintain trust and performance. Information systems security administrators must safeguard their systems and information assets against the possible threats posed by insider crimes (Saxena et al., 2020). According to Bunn (2023), IS security administrators must remove any environmental opportunities that could be interpreted as a window for insiders' malevolent attempts. Organizations have implemented two primary approaches to deter

employees from carrying out insider attacks: (1) raising employee awareness and (2) using methods to decrease the likelihood of criminal activity (Alsowail & Al-Shehari, 2022). Administrators of IS security should also reduce the incentive of their staff to commit insider crimes (Alsowail & Al-Shehari, 2022). Thus, administrators of information security must concentrate on raising expenses and lowering the expected advantages of hostile actions (Alsowail & Al-Shehari, 2022). By focusing on physical obstacles, access control, and technological monitoring and surveillance rather than only dealing with insiders' internal motivations, this security approach lessens the likelihood that hostile insiders would implement their plan (Jeong & Zo, 2021). There is a need to balance the impact of the controls with the enhancement of employee responsibilities and job specifications.

Overly restrictive policies may weaken trust and ultimately reduce the effectiveness of insider threat mitigation. Sometimes, organizational strategies can violate the personal space of every worker (Hodgins et al., 2020). Employee-employer relationships built on mutual trust may be weakened because of the increased limitations placed on each person's activities (Katou et al., 2020; Soltani & Wilkinson, 2020). Moreover, because the bargaining power is tilted clearly in favor of the employers in this bilateral relationship, it may be highly disadvantageous for employees to be compelled to adhere to the dictates of organizational policy (Fornell et al., 2020). The limitation has also impacted the freedom of employees within the organization. Even though the employees are fully aware of the policy encroaching on the aspects of their privatized space, most of the employees have been made to surrender their rights to privacy despite

the lack of any apparent problems with the procedures (Saxena et al., 2020). Jeong and Zo (2021), Padayachee (2022) and Saxena et al. (2020) pointed out that these responses could pose a negative effect on organizational interventions aimed at decreasing the probability of malevolent insider involvement in a criminal act. Therefore, there needs to be more knowledge of the negative impacts of the opportunity-reducing approach in countering insider threats (Jeong & Zo, 2021) to reduce exposure and enhance adherence by implementing adequate controls. Business leaders should consider organizational control mechanisms not as a tool of domination but as collaborative frameworks.

Understanding how mitigation controls established by management support employee performance is key to their acceptance. Employers should develop a more structured and balanced system whereby the controls established to reduce and mitigate the threats do not discourage or demotivate employees in the performance of their duties, but rather make employees see the control as a requirement necessary to perform their duties (Uchendu et al., 2021). A study by Blanuša et al. (2021) on the moderating effects of perceived job uncertainty found that employees feel more pressured to leave their current positions if they feel uneasy about their jobs. To remedy the degree of discrepancy in bargaining power between employers and employees is one of the leading possible causes of the negative effect; it is imperative to comprehend and proactively manage the factors that have the potential to exacerbate the bargaining power disparity in bilateral interactions (Jeong & Zo, 2021). Poorly designed control systems can worsen employee anxiety if job uncertainty and power imbalance exist. The impact of the global pandemic of 2019 has contributed immensely to the growth of cyberactivities.

The surge in online activity, public anxiety, and digital commerce created conditions that increased cybercrime globally during the COVID-19 pandemic. The COVID-19 pandemic has also resulted in unique cybercrime-related activities that have affected businesses (Lallie et al., 2021). The COVID-19 pandemic has caused a growth in the internet/digital world, resulting in an increase in the volume of ecommerce transactions all around the world (Weil & Murugesan, 2020). According to Kumar et al. (2022), the pandemic heightened public anxiety, consequently increasing the number of cyberattacks, and the likelihood of its success. Lallie et al. (2021) suggested that opportunistic attackers may launch their attacks during major public events, ongoing crises, or natural disasters to maximize their gains. The number of malware attacks, phishing attacks, and online scams has increased significantly since the start of the COVID-19 pandemic (Weil & Murugesan, 2020). There is a need for cybersecurity awareness, policy intervention, and individual behavioral change to help reduce cyberattacks on business enterprises.

The COVID-19 pandemic increased the online activity and data exposure to cybersecurity risks. The COVID-19 pandemic has caused unprecedentedly high unemployment rates (Blanuša et al., 2021). The increase in transactions between buyers and sellers online has also increased the personal and financial details of individuals (Kumar et al., 2022). The increase in this information on the internet can serve as an opportunity for hackers and fraudsters to defraud innocent and careless individuals (Lallie et al., 2021). The effect of the pandemic has necessitated the utilization of the self-efficacy criteria to predict the intentions and behavior of people towards protection

against any attack (Marina & Simone, 2023), by using technology to control and reduce exposures to risks. The data exposure, therefore, requires employees to rely on self-efficacy and technology to protect them.

Cybersecurity Compliance in Organizations

Due to the increase in technological advancements, exposure to cyberattack among organizations has risen to 67% (Tushar, 2025). The exposure has caused employers to utilize adequate strategies of threat perception, benefits, costs, and other factors to help increase awareness, thereby improving the level of protection of organizational data by employees (Li et al., 2022). In addition to adopting protective measures such as encouraging positive behavior of employees, businesses must disseminate information relating to the risks and punishments associated with misapplying or not following an organization's cyberpolicies (Hansen et al., 2023). Employee compliance may help militate against or eliminate these hazards (Chen et al., 2022). Wong et al. (2022) described compliance intention as the employee's willingness to safeguard organizational assets from security breaches and fulfill their roles in the organization. Evaluated constructs related to compliance and behavioral intent toward adhering to policy guidelines include role values, reactance, neutralization, habit, response efficacy, and threat (Koohang et al., 2021; Y. Lee, et al. 2023; Shaikh & Siponen, 2023; Wong et al., 2022). Enlightening employees on the need for compliance can help to improve the risk mitigation activities of the organization.

Knowing the intentions of employees can help to understand how best to implement the necessary controls. The employee's roles in protecting organizational

resources are usually emphasized in the organization's security policy (Wong et al., 2022). However, compliance with these policies and rules depends on the employee's motivation to conform (Wong et al., 2022). Human nature may also affect the way employees adopt and comply with cybersecurity rules established by an organization (Li et al., 2019). Organization-specific information security requirements should consider whether employees perceive deterrents and are motivated to comply with security policies (Alraja et al., 2023). Other areas of concern include external pressure and internal motivation that enhance adherence to security regulations among employees, and the degree to which the employee is interested in following the firm's policies (Corallo et al., 2020; Jaeger et al., 2021; Wang et al., 2022). Additionally, various motivating variables may influence compliance behavior (Chen et al., 2022). Understanding what motivates employees can help businesses implement adequate training for effective compliance.

Traditional cybersecurity training and policies alone may not effectively influence employee behavior, as compliance is shaped by deeper psychological, emotional, and social factors. Numerous studies on cybersecurity (Hina & Dominic, 2020; Li et al., 2019) have reported that some security policies may not be effective for employees. Some employees may also be unaware of their organization's security policies or underestimate information security risks (Li et al., 2019). Additionally, other studies found that employees who had been exposed to the required standard of cybersecurity training from their organizations did not exhibit greater levels of cybersecurity behavior compared to the control group (Li et al., 2019). These findings can be explained by the

findings of D'Arcy and Lowry (2019), whose model of employee compliance with information security policy includes cognitive beliefs on the consequences of compliance and noncompliance, state-based affective constructs such as work-impediment events and mood, normative influences, and moral considerations regarding employee compliance.

Compliance can also be affected by influences unrelated to behavioral trends. Thus, any model or theory on security compliance should capture and explain the variance in daily affective constructs (D'Arcy & Lowry, 2019). Noncompliance with a business's security policy creates system vulnerabilities and endangers the organization's resources (Koohang et al., 2021). However, cybersecurity breaches caused by employees have become commonplace in organizations and are expected to increase further (Vance et al., 2020). Khatib and Barki (2020) suggested that the universal incidence of employee-generated information security transgressions is very high. Published data also indicates an increased risk to information security and that most leaks occur due to non-compliance with organizational guidelines (Wong et al., 2022). As a result, organizations should implement and ensure adequate compliance with security measures established to protect against risk exposure.

Strategies in Employee Training for Militating Against Cyberattacks and Threats

Cyberattacks and threats may cripple an organization's operations. Wilson et al. (2023) suggested that the consequences of mishandling insiders with access to confidential information include loss of intellectual property and confidential data, blocked sales, severed communications, reduced data integrity, and damaged information assets. Thus, to protect against cyberattack, business leaders should develop a well-

defined cybersecurity awareness culture to help and encourage employees to understand and implement safety in their dealings with the internet (Shaban et al., 2023). Due to the increase in the cost of cyberattack and their frequency, training is essential to help businesses implement adequate strategies for protecting their business assets (Shaban et al., 2023). Understanding how training can help improve the safety capacity of employees is necessary for organizational consideration.

Training is important within an organization to help in disseminating information and ideas to employees. Training results in the transfer of knowledge and skill from experienced and knowledgeable individuals to new or inexperienced employees (Butavicius et al., 2022). Training will also ensure that employees are aware of threats and the training will help their response to them (Chowdhury et al., 2023). Level of education is not linked to security awareness behavior and hence requires training at all levels to combat and detect attacks (Butavicius et al., 2022) Due to the evolution in the digital world and the exposures of business systems to various risk patterns, it is important to identify various training strategies that can be used to disseminate information to employees to address the growing gap in the required cyber- and digital security capacity and capability (Nweke et al., 2022). The location of sensitive data and information is also part of the safety features that organizations need to display or implement.

A robust insider threat mitigation strategy depends on the ability to accurately identify and categorize IT assets to enable the application of proper security controls. As part of a mitigation program, every IT resource currently in use needs to be located and

inventoried (Clifton, 2024). This is because managing insider threats requires awareness of where sensitive or vital data is processed and kept (Clifton, 2024). However, this procedure might be challenging for businesses using a hybrid or multi-cloud infrastructure (Clifton, 2024). Data assets can be categorized after they have been identified to help provide the appropriate level of protection for them (Khando et al., 2021). Categorization of data involves the classification of data according to different conditions to enable identifying their importance, risk condition, and exposure capability (Baldissone et al., 2019). Privileges will then be given to the data after categorization. Particular sorts of information need to be handled differently, or access must be strictly limited to accounts with specific privileges (Baldissone et al., 2019). Accurate categorization of newly ingested information is also necessary to guarantee that it receives the attention required at all levels of the organizational structure (Cremer et al., 2022). Adequate sorting of data directly reduces the opportunity for both internal and accidental insider breaches through the handling procedures of sensitive data to authorized personnel.

Organizational leaders need to explicitly define the safety roles of employees at the early stages of employment. Understanding the role of employees can help give them a self-belonging and the willingness to protect the organization's information against cyberattack (Stacey et al., 2021). Using PMT, it was identified that adequate training of employees in cyberattack concepts has improved cybersecurity awareness in the organization and has also helped employees to protect themselves by adopting positive behavior and avoiding any negative result or impact of non-compliance with the relevant

controls (N. F. Khan et al., 2023). Using different training techniques can help employees understand security measures and how to safeguard the business against cyberattack.

Training can be carried out using different formats and methods. Some of the methods of training in cybersecurity include

- lecture based training: This type of training involves the use the delivery of information by an expert in the field of study to recipients in a classroom environment where employees are actively present at a time (Alnajim et al., 2023). Students are actively engaged during classroom interactions and require instructors with adequate expertise and knowledge for it to be successful.
- films and video-based training: This type of training involves the use of films and videos to educate employees. This type of method is good for use to teach employees on the fundamentals and the principles of cybersecurity and how to protect against attacks (Rana et al., 2021).
- technology-based learning: This is a training method where trainings are held online by the trainees using a computer system and provide a platform for conducting exercises and test using cyberranges (Katsantonis et al., 2023). This system allows for high number of patronage and participants as well as enable trainees to study at their own pace.
- simulation training: This involves the use of augmented reality (AR) and virtual reality to create a realistic situation for the test or use of skills and its application. Simulation training helps to enhance decision taking (Walls et al.,

2024). It can be used to help in prediction of outcomes of cyberattack and actions to take to prevent them in a training setting.

- **game based training:** This approach uses computer games to disseminate learning to participants. It allows users to access information and implements different theories and concepts of cybersecurity compliance (Van et al., 2021).

The training of employees by organizations can help to expose them to the impact of their actions on the activities of the organization, the dangers of phishing attacks, and ways to identify them. Security training awareness programs can be developed by organizations to build and impact the way individuals react and comply with cyberattack and threats (N. F. Khan et al., 2023). According to N. F. Khan et al. (2023), training programs are effective in helping individuals to protect themselves and the resources of their employers and to create awareness towards cybersecurity attacks.

Creation of an Organizational Data Handling Policy

The requirement for an organization to safeguard its data from unlawful or external exposure has resulted in the creation of an organizational data management policy. The data handling policy will serve as the cornerstone for further countermeasures against insider threats (Khando et al., 2021). The project will help to appreciate the dire need to address the issue of employee training in the fight against cybersecurity compliance threats from insiders (Alsowail & Al-Shehari, 2022). Emphasizing the findings, the results of the research based on TQM principles show how concepts such as continuous improvement, leadership's commitment, and the education of the employees can improve immunity against insider threats (Alsowail & Al-Shehari, 2022). Another

advantage of proper training is that employees become prepared to notice threats and act according to the planned procedures while creating a security-friendly environment.

Adequate training help the employees to understand their role of identifying any threat to the organization information system as quickly as possible and using the organization established procedures/ guidelines to notify senior management of such threats before they impact the business activities negatively thereby jeopardizing the high cost of investments by organizations to protect their information and data assets (Wilson et al., 2023). Timeliness and consistency of training can also be considered by organizational leaders.

Regular updates, psychologically informed training, and continued research into long-term effectiveness across varied organizational settings can help to strengthen cybercompliance. H. Lee (2021) also clearly indicated the need for frequent reviews of training programs and includes psychological and behavioral aspects so that companies provide their employees with a top-notch and enhanced training system to prevent cybersecurity compliance relapses. In addition, Khando et al. (2021) stressed that more research should be done about integrated references in connection with the conception between the security needs of the organizations and the Employee Assistance Programs, especially in the era of economic challenges. However, Shapira (2022) discussed that the long-term effects of the training interventions and the effectiveness of contextualized training interventions across multiple organizational settings still need to be determined. Thus, future studies should focus more on these suggestions to address the issue of inside threats more effectively.

Emphasis on Employee Training and Responsibility

Understanding the responsibilities of employees and how to protect data can be improved through adequate, comprehensive, and targeted training. To ensure employees know how to use the company's information assets, employees should receive training on the data management policy (Jeong & Zo, 2021). Employees should receive security awareness training, which educates them to recognize phishing scams and other types of social engineering and helps to stop sensitive information from inadvertently being disclosed (Clifton, 2024). Users ought to be aware of the data they have access to and how to use it without endangering it. As part of an efficient insider threat program, all employees should understand their role and responsibilities in safeguarding firm data against insider threats, whether deliberate or accidental (Fornell et al., 2020). Appropriate training can lower the likelihood of errors and detrimental behavior, including emailing files containing private information (Fornell et al., 2020). Whenever feasible, it is always better to prevent the error at its source (Alhayani et al., 2021). Understanding the employee age bracket can also help to implement adequate training to counter cyberattack.

Age factors can also play an important role in the type of training that employees may need to be exposed to for protection against cyberattack (Daengsi et al., 2022; Li et al., 2022). Categorization of employees into different groups, such as baby boomers (1945-1964), generation X (1965-1979) and generation Y (1980-2000), will help to identify specific training for each of the categories and help the organization develop adequate training for each group (Redekop, 2021). However, a research on Thai

employees by Daengsi et al. (2022) found that there were no significant differences in cybersecurity awareness among Baby Boomers, and Generations X and Y. Similarly, Aldawood and Skinner (2019) found that using case studies and case scenarios in training and awareness programs enabled users of all ages to freely use technology due to an enhanced knowledge base of potential gaps that hackers may take advantage off. The training should be continual due to the dynamic nature of the cyberworld and the continuous threats and attacks by cybergangs and traitors who disrupt business activities through cyberattack (Montasari, 2024). The training may also enable businesses to develop high-level policies that will assist employees in managing any cyberthreats that may be encountered by the organization.

Monitoring and Management of Anomalous Behavior

The behavior of employees can expose a business to security risk. To successfully reduce the danger of both external and insider threats, abnormal behavior must be observed (Fornell et al., 2020). An intentional insider threat may be indicated, for example, if someone persistently attempts to access prohibited content or participates in other potentially harmful behavior (Alawag et al., 2023). The person who violated the rules can be informed that their actions have been recorded and will be watched over more carefully in the future (Alawag et al., 2023). Intentions for committing violations against the organization can also be identified to enable the review and improvement in controls that may reduce those intentions (Dearden et al., 2023). The person could only require more instruction on the data handling policy. This training can be conducted interactively when an anomaly is discovered through contemporary insider threat

prevention software systems. According to Schneider et al. (2021), fear can play a major role in cyberattack by causing individuals to take actions against their wishes or act irrationally. As a result, the fear appeal model will consider exposure of how to identify the fear early and develop training that can help to build up their confidence in taking actions against the attacks (Schneider et al., 2021). It also helps to develop processes that can help to reduce any negative actions by those responsible (Schneider et al., 2021). Business leaders need to address insider threats and behavioral anomalies to ensure adequate cybersecurity risk mitigation.

Research Gap

The existing research shows several gaps concerning employee training as a way of dealing with insider threats to cybersecurity compliance. First, there are a significant number of articles that pay attention to general training practices; at the same time, there is a deficiency of many articles that focus on the research of these programs and their efficiency in cybersecurity (Khando et al., 2021; McLlwraith, 2021; Safa et al., 2019). Responding to the lack of research on the effects of involving continuous and updated training programs customized to different and new threats, the following hypothesis of the current project is developed.

Conclusion

This project highlights the need to address the issue of a lack of strategies by organizational leaders and cybersecurity professionals in the fight against cybersecurity compliance threats from insiders. Emphasizing the findings, the results of the research based on PMT principles may show how concepts such as continuous improvement,

leadership commitment, and the education of employees can improve immunity against insider threats.

The literature review also indicated the need for frequent reviews of the training programs, including psychological and behavioral aspects, so that companies provide their employees with a top-notch and enhanced training system to prevent cybersecurity compliance relapses. In addition, it stressed that more research should be done about integrated references in connection with the conception between the security needs of the organizations and the employee assistance programs, especially in the era of economic challenges. However, the following research limitations are noted: the long-term effects of the training interventions still need to be determined, and the effectiveness of contextualized training interventions across multiple organizational settings had not been determined.

Transition

In this section, I reviewed the various literature discussing the factors and emergence of cyberattack and how the threats posed by the attacks can be managed using training as a major instrument to empower employees to be able to take accurate and precautionary actions to protect business assets. I also discussed the impact of PMT, which considered the factors that will help employees adhere to the set controls by businesses. The TQM theory also ensures the continuous improvement of business processes to help establish controls for effective cyberprotection and safeguarding business operations and company assets in the long run. In section 3, I discussed the methodology used in the research project, focusing on the nature of the project,

population, and the sampling techniques used to select the participants. The data collection techniques and the interview questions will also be discussed as they relate to the organization and the analysis of the data. In Section 4, the findings of the project will be discussed.

Section 3: Research Project Methodology

In this section, I provide details on the methodology of the research project. I outline the ethical considerations, project design, population, sampling techniques, data collection activities, and analysis methods. The goal was to identify and explore effective strategies some cybersecurity leaders use to improve employee cybersecurity compliance to increase business profitability. This section also includes discussion of reliability and validity concerns that I addressed to ensure the rigor of the project.

Project Ethics

As the researcher, my role in the data collection process was to ensure that all research activities align with ethical standards and guidelines, maintaining integrity and compliance with institutional regulations. Participants were provided with an informed consent form to guarantee they fully understand the projects purpose, procedures, and any potential risks before deciding to participate (see Pietrzykowski & Smilowska, 2021). Emphasizing voluntary participation ensured individuals join the research willingly, while allowing them to withdraw at any time to protect their autonomy and well-being (see Josephson & Smale, 2020). Measures were taken to safeguard participant identity and responses, ensuring confidentiality and minimizing privacy risks. Additionally there was no coercion or incentives, ensuring that participation were based on genuine willingness rather than external pressures, ultimately enhancing the reliability and ethical integrity of the research (see Josephson & Smale, 2020). Genuine willingness of participants helped to give credibility to the results of the research project.

To ensure confidentiality, I did not disclose any names or identifiable information of individuals or organizations. Data will be securely stored for 5 years in compliance with research ethics and Walden University guidelines. My interest in the project was based on the need to reduce business losses due to risk of exposure to cyberattack. As the researcher, there was no relationship with the respondents apart from the sole purpose of obtaining opinions and views for the sake of the project. My role was solely that of a researcher, and I approached the study from a neutral perspective to minimize the risk of bias and ensure that my interpretations and conclusions are based solely on the data collected. I will remain aware of any potential assumptions or preconceptions I may hold due to my prior knowledge of the field and will use strategies such as member checking, reflective journaling, and peer debriefing to uphold objectivity and trustworthiness throughout the research process. I waited until I received Walden University Institutional Review Board approval (no. 08-04-25-0337123) before conducting the project.

Nature of the Project

This project featured a qualitative pragmatic design. Qualitative research is an exploratory approach that seeks to capture information on complex social phenomena (Lim, 2024). Unlike quantitative methods that measure predefined variables, qualitative research allows for open-ended inquiry, making it suitable for examining human behaviors, decision-making processes, and contextual factors (Hammoumi et al., 2024, Lim, 2024;). This project employed a pragmatic inquiry design, which prioritizes real-world problem-solving and practical application of knowledge. Pragmatic inquiry enables

flexibility in data collection and analysis, allowing the researcher to adapt the project based on emerging findings (Huising & Silbey, 2021; Ramanadhan et al., 2021). The flexibility helped to obtain more information from the participants, hereby enabling more valid and reliable project results.

A qualitative approach is suited for the project as it facilitated exploration of cybersecurity leadership strategies in promoting employee. Since cybersecurity compliance involves both technical policies and human behavior, a qualitative method allows cybersecurity leaders to share their real-world experiences, insights, and best practices. Additionally, the pragmatic design ensures that the findings are directly applicable to organizational settings (Huising & Silbey, 2021). The design makes this project valuable for cybersecurity professionals seeking to enhance compliance and increase business profitability. The design also gave the participants more freedom to discuss their success strategies with respect to the research topic.

Population, Sampling, and Participants

The target population for this project was cybersecurity leaders who have successfully managed and implemented compliance and risk management strategies within their organizations. These individuals had direct experience in developing, overseeing, and enforcing cybersecurity policies to mitigate risks and ensure regulatory compliance (see Muzari et al., 2022; Subedi, 2021). I identified and selected a sample of cybersecurity leaders who have demonstrated success in managing and implementing compliance and risk management strategies to increase business profitability. The

selected participants included managers, executives, and other key decision-makers responsible for cybersecurity policies and risk management within their organizations.

The sampling method that was used in this project is purposive sampling. Purposive sampling is a non-random sampling technique where participants are selected based on their knowledge, experience, and relevance to the research topic (Robinson, 2023). This method is appropriate for qualitative research as it ensures that participants can provide rich, detailed, and meaningful insights related to the project research question. I used purposive sampling to identify qualified participants. Additionally, I applied purposive sampling to select participants who have direct experience with cybersecurity compliance strategies and can effectively articulate the challenges, best practices, and strategies associated with their implementation.

A sample of six qualified respondents was required. This number of participants was guided by the principle of data saturation, where data collection continues until no new insights emerge from additional interviews (see Braun & Clark, 2019). This number is justified because the study aims to gain in-depth. Each participant was selected based on their ability to provide meaningful, experience-driven insights into cybersecurity compliance and risk management strategies. The current number of participants was enough to achieve saturation and as a result, there was no need to recruit more participants as saturation was achieved, ensuring that the findings comprehensively capture the perspectives of cybersecurity leaders on compliance and risk management strategies. The participants were identified as professionals who have worked in Information Security and compliance roles who have more than 5 years of experience.

The selection process involved requesting emails to prospective participants using professional sites such as LinkedIn or by personal reference.

Data Collection Activities

Data was collected using semistructured interviews. I began by identifying individuals with relevant experience in cybersecurity roles and connect with them. These individuals were screened to ensure they met the inclusion criteria. Once the qualification criteria had been met, an open flyer invitation emails were sent to identify prospective participants. Once invitations were sent, willing participants responded via email or in person, and then I obtained their informed consent. Following the interview protocol (see Appendix A), I then conducted semistructured interviews to collect data from participants. I used capabilities of the Zoom videoconferencing platform to record the interviews. Before recording, I explained the purpose of the recording and how the data would be securely stored and used. In addition to audio recordings, I took handwritten notes to capture key points. To safeguard against data loss, I created multiple backups, including encrypted digital copies stored on a secure, password-protected drive.

After securing consent, I scheduled each interview at a convenient time. During the interview, each interview lasted approximately 25 to 40 min and took place through Zoom calls depending on participant preference timing. I used open-ended questions to encourage the participants to share their experiences and insights. After obtaining the participants' consent, I audio-recorded the interviews for accuracy and transcription purposes.

I transcribed the interviews verbatim and verified the accuracy of the transcripts. I employed member checking to review and clarify participant's responses to ensure their views are accurately represented. I then organized the data systematically and coded the data using thematic analysis techniques. I stored all interview data securely and maintained confidentiality throughout the research process. Finally, I analyzed the findings and prepared them for presentation in the final research report.

Interview Questions

I developed the interview questions based on my own experience, a thorough review of the literature. My background guided the formulation of questions that were relevant to cybersecurity compliance strategies. Drawing from my experience, I had constructed questions that explored practical challenges, effective solutions, and leadership strategies in managing cybersecurity risks to increase business profitability. Additionally, I had incorporated insights from scholarly literature to ensure that the questions align with existing knowledge while allowing room for new findings.

The interview questions (see also Appendix B) were as follows:

1. What are the key cybersecurity compliance threats your organization currently faces?
2. What strategies do you use to foster a culture of cybersecurity awareness and accountability to improve profitability?
3. How do you assess the effectiveness of cybersecurity training programs in reducing compliance risks?

4. What role does leadership communication play in reinforcing cybersecurity training outcomes?
5. How do you measure the return on investment (ROI) of cybersecurity training initiatives?
6. What challenges do you encounter when trying to align training programs with compliance goals?
7. What training delivery methods (e.g., e-learning, in-person, simulations) do you find most effective in cybersecurity compliance and why?
8. How do you ensure continuous improvement in cybersecurity training content and delivery?
9. In your opinion, what are the most important elements of successful cybersecurity training?
10. Is there anything else you'd like to share on this topic?

Data Organization and Analysis Techniques

After the interviews were completed, the data were organized and analyzed. I employed Braun and Clark's (2006) six-step thematic analysis process to ensure a systematic and rigorous approach to data interpretation. The first step, familiarization with the data, involved reading and rereading the interview transcripts to immerse myself in the responses and understanding of the content. This process allowed for initial observations and patterns to emerge while ensuring that no significant details are overlooked (Fuchs, 2023). In this step, I developed a sense of key ideas and recurring topics that later formed the basis of thematic coding. During this stage, I also took

preliminary notes on potential areas of interest, helping to lay the groundwork for the subsequent steps in the analysis.

The second step, generating initial codes, involved systematically identifying meaningful segments within the data that are relevant to the research objectives (see Locke et al., 2020). I used both Microsoft Excel and manual coding methods to enhance accuracy and reliability. I also made use of copilot to confirm some of the themes I identified from my initial source. The Microsoft excel assisted in organizing large amounts of qualitative data efficiently, allowing me to label and retrieve coded segments quickly. Simultaneously, manual coding provided flexibility and deeper engagement with the data, ensuring that nuanced themes are not overlooked. Once initial codes were established, I proceeded to the third step, where I organized the codes into broader themes that reflect patterns across participants' responses (see Ramanadhan et al., 2021). This process involved grouping related codes to create overarching themes that provide insight into cybersecurity leadership strategies for improving employee compliance.

Following theme identification, the fourth step, reviewing themes, required refining the themes by ensuring they accurately represent the data and eliminating redundant or weakly supported themes (see Ramanadhan et al., 2021). During this stage, I revisited the transcripts and assessed the coherence and consistency of each theme. The fifth step, defining and naming themes, involved articulating what each theme represents and how it contributed to answering the research question. This step ensured that the themes were meaningful, distinct, and grounded in the data. Finally, I synthesized the findings into a cohesive narrative in the report-writing stage. This involved integrating

the themes with existing literature to provide context and support for the findings (see Ramanadhan et al., 2021).

Reliability and Validity

Reliability

Building trust and adequacy of the results is important in any research study. Ensuring trustworthiness in qualitative research is essential for maintaining the credibility, transferability, dependability, and conformability of the study findings (Ahmed, 2024). To address reliability, I used member checking, which allowed participants to review interview transcripts and confirm the accuracy of interpretations. This step not only increased participant engagement but also enhanced the integrity of the findings. Transferability was achieved through thick description, allowing readers to determine the applicability of findings in different contexts. To ensure dependability, I maintained an audit trail documenting data collection methods, coding steps, and analysis decisions. Lastly, I enhanced conformability by keeping a reflexive journal to identify and reduce researcher bias. Without proper measures to ensure trustworthiness, the project's conclusions may be questioned or deemed unreliable (Adler, 2022). Trustworthiness will therefore require avoiding personal bias, using accurate data, and ensuring the results are applicable to the scope of the project.

Validity

The acceptance of the research project, based on the facts obtained, is an important aspect of any project. Validity refers to the confidence in the truthfulness and accuracy of the findings (Adler, 2022). To achieve validity, I used member checking, to

enhance the credibility and validity of the findings for accuracy before data analysis. This strategy ensured that responses were correctly interpreted and that participants' perspectives were authentically represented. Engaging with participants during the validation process also created an opportunity for clarification, allowing the participants to elaborate on their responses if necessary. Through these efforts, I enhanced the credibility of the research by ensuring that the data accurately reflects the participants' experiences and perspectives. To achieve data saturation, I ensured that participants were well knowledgeable about the topic of the project. Data saturation was achieved when no new information or insights relevant to the research question were obtained from new data.

Transferability concerned the extent to which the findings can be applied to other contexts or populations (Drisko, 2024). To enhance transferability, I provided rich, detailed descriptions of the research setting, participant characteristics, and findings. Dependability ensured that the research process was consistent and repeatable (see Haq et al., 2023). To establish dependability, I maintained a detailed audit trail that documents all methodological decisions, coding processes, and theme development throughout the project. This audit trail allowed other researchers to follow the steps taken in this project, ensuring transparency and methodological rigor. Lastly, conformability addresses the objectivity of the research findings by minimizing personal bias (see Lim, 2024). I achieved conformability through reflexivity, keeping a research journal to document my thoughts, assumptions, and potential influences on the analysis. This self-awareness will

help ensure that personal biases do not influence my results, allowing for a more objective and reliable interpretation of the data.

Transition and Summary

In this section, I outlined the research methodology, including ethical considerations, study design, population, sampling techniques, data collection activities, and analysis methods. In the project, I employed a qualitative pragmatic design to explore effective cybersecurity leadership strategies for improving employee compliance to increase business profitability. Participants were cybersecurity leaders selected through purposive sampling, and data was collected via semistructured interviews. Braun and Clark's (2006) six-step thematic analysis was used to analyze the data, ensuring a systematic approach to identifying key themes. To enhance trustworthiness, I implemented credibility, and transferability, dependability, and conformability strategies throughout the research process.

Section 4: Findings and Conclusions

The project featured a qualitative pragmatic inquiry design. The purpose of this qualitative inquiry was to identify organizational leaders' effective strategies for using training to mitigate threats to cybersecurity compliance. The project involved extensive research on topics that included cybersecurity, compliance, training, and leadership behavior. The increase in cyberattacks on business organizations and the impact of a successful attack have prompted the need to undertake this project.

In the project, I employed a purposive sampling method to identify participants who had experience and exposure to cybersecurity threats or held leadership positions in their field of expertise. A sample of six participants were selected, and I conducted interviews with each participant after obtaining consent to participate in the research project. The guiding research question for this qualitative pragmatic inquiry project was, What effective strategies do some cybersecurity leaders use to improve employee cybersecurity compliance and increase business profitability? I began the data collection process after obtaining approval from the Walden University Institutional Review Board (approval no. 08-04-25-0337123), in accordance with institutional requirements. The interview questions consisted of 10 open-ended questions for participants to explore their experiences on the topic of the project.

Presentation of the Findings

The purpose of this qualitative pragmatic inquiry project was to explore effective strategies organizational leaders use to mitigate threats to cybersecurity compliance. Many organizations are facing exposure to cybersecurity threats due to their online

business transactions. The emergence of the Internet and the need for business activities to be carried out at different locations and in extended geographical settings have resulted in business leaders needing to invest in information technology infrastructure for business sustenance. The research question underpinning this project was, What effective strategies do some cybersecurity leaders use to improve employee cybersecurity compliance to increase business profitability?

To answer the research question, I conducted semistructured interviews with six cybersecurity compliance experts to gather more information about their experiences with the project topic. I obtained additional data from other sources, including the Internet and relevant past projects related to the topic. The conceptual framework for this qualitative, pragmatic inquiry study aligns with the PMT and the TQM framework. The PMT was developed in 1975 by Rogers, while TQM was created around the 1980s by numerous theorists, including Edward Deming, Joseph Juran, and Philip Crosby. During the course of obtaining data from the participants, I achieved data saturation after interviewing the fourth participant. However, the interview continued with two additional participants, as per the project proposal, to identify any further themes that might arise from the project topic.

Data saturation in qualitative research was achieved when no new themes or information emerged from additional data obtained from any new participant. To ensure the proper tracking of participants and maintain confidentiality, I assigned each participant a unique number from P1 to P6. I conducted the interview using the Zoom videoconferencing platform, with the meeting link sent to each participant after they

confirmed their willingness to participate in the project. The use of Zoom also enabled me to connect with the participants remotely and at their convenience. The sessions were audio-recorded after confirmation from each participant, and the audio recordings were summarized using the Copilot tool, in addition to the notes taken from the recordings. At the end of every session, I conducted adequate member checking procedures by ensuring that the data collected were properly documented using Microsoft Word and sent back to each participant to confirm the accuracy of the documentation in relation to their thoughts, views, and experiences shared during the interview session. The feedback obtained from the six participants during the interview session provided me with the opportunity to validate the data and further ensured the trustworthiness of the findings. The feedback also lent credibility to the project by confirming that the information captured accurately reflected the participants' views, and no additional information was included from the participants in the report.

After obtaining data from the participants, I analyzed the data using Braun and Clarke's (2006) six-phase model of thematic analysis to identify key themes, thereby supporting data triangulation from industry documents. The Braun and Clarke's (2006) six phase model involved the familiarization with the interview response data through the verbal transcribing and interpretation of the participants interview responses accurately, generation of codes from the data, searching for and identifying themes and subthemes, reviewing of the themes and subthemes for accurate and proper consolidation into groups, defining and naming the various themes and the production of the report. After analyzing and verifying the data, I identified eight themes as follows: (a) leadership

involvement, (b) training effectiveness, methods, and challenges, (c) customized training strategies, continuous improvement, and expert collaboration; (d) human factor influence in cybersecurity and emerging technology; (e) key cybersecurity threats, (f) cybersecurity awareness strategies, (g) compliance and regulatory alignment, and (h) return on investment on training. Each theme is discussed below.

Theme 1: Leadership Involvement

The first theme to be discussed is the leadership role in controlling behavior pattern of employees and their influence on attitudes toward cybersecurity compliance. Leadership spans various levels of the organization, and each level should maintain relevance and provide adequate training. Leadership needs to implement strategies to define and encourage a culture of safety and eagerness to learn among employees, thereby protecting the organization against cyberattacks. Employees are motivated by an adequate reward system that enables them to utilize training for effective cyberattack controls, leveraging the knowledge gained, as well as sufficient exposure to real-time experiences.

According to P2, leaders can use sanctions and compliance enforcement against employees who fail to abide by the business's cyberpolicies or protect the organization against cyberattack. Business and organizational leaders need to define the requirements for employees in their day-to-day activities. P3 stated that, "There is need for leadership to develop mandatory training and participation at all levels of leadership, with adequate follow-up from top management to ensure employees are well-cultured and adequately knowledgeable in protecting the organization against cyberattacks." P4 and P5

recognized the concept of leadership by example, a situation where leadership exhibits interest and informed participation in training programs, as well as helping junior employees to identify and understand the implications of their actions, both in the short and long term, while also showing support where necessary, which will help to build confidence and trust among employees towards adequate protection. According to P6, “Leadership should also ensure that sufficient resources are allocated for training programs, both in terms of financial and human capital, by employing professionals who can effectively drive business strategic direction.” Overall, leadership is the originator of building a culture among employees, giving credibility, and ensuring adequate access to necessary resources.

Theme 2: Training Effectiveness, Methods, and Challenges

Training effectiveness refers to the ability to assess the impact of training on business processes. According to the overall responses from participants, measuring the effectiveness of training can be challenging due to its dynamic nature. P1, however, identified that to measure the efficacy and impact of training, it should establish a system where pre- and post-behavioral or activity changes can be measured effectively by leadership. This identification will help to identify the logical impact of the various training sessions on employee behavior. P1 stated that, “The measurement pattern training strategies will also impact the behavior of employees towards cybersecurity training, which will help improve and reduce cybersecurity attacks on organizations.”

Using key driving tools to measure behavior patterns, participants identified various approaches for implementation. P2 and P3 identified simulated attacks,

penetration tests, surveys, and phishing tests to assess the practical understanding of multiple attacks among employees and measure the impact of various training programs developed by the business, specifically whether they have a positive effect on the business.

According to P1, “A continuous feedback system should be developed where employees can advise on how the various training sessions developed by the organization have been helping them understand and mitigate the impact of risk and exposure to threats.” P1 and P6 identified the use of pre- and post-training assessment techniques, which enable employees to identify and evaluate the effects of the training in combating cybersecurity attacks on the business. P5 and P6 also identified incident tracking and incident reporting techniques to help identify areas of business exposure, enabling businesses to focus more resources on those areas. When considering training methods, participants explored various options to help employees understand and learn more about the cybersecurity environment. P1, P2, P3, and P6 identified the in-person, instructor-led training methods. P4 identified the use of infographics and simulation learning methods. According to P5, “Self-paced hands-on experience training should be developed for employees to enable them to learn at their own pace.” The response from the participants confirmed that the effectiveness and method of training have a positive alignment with how employees can help protect the organization against cyberattack.

Theme 3: Customized Training Strategies, Continuous Improvement, and Expected Collaboration

According to all participants, effective cybersecurity begins with employee awareness. Employee awareness can be better understood through the use of effective strategies that help employees understand the need for a proper control structure, which can be achieved through targeted training. According to P5 and P6, real-world simulations can help employees experience a real-world scenario in a testing environment, thereby enabling them to experience and build more confidence as they encounter real-world scenarios. According to P1 and P6, workshops and customized training can be developed for different departments, all with the same final goal of reducing exposure to threats from cyberattacks. Training strategies for participants should be continuous, engaging, and role-specific to ensure the early dissemination of knowledge about risks and controls, from the lowest to the highest levels of organizational leadership.

As confirmed by P2, “There is a need for spot checks and phishing tests to be introduced by management to enable employees to maintain a steady knowledge and understanding of the risks they are exposed to.” The use of continuous improvement and training programs will also help maintain steady expertise and exposure to new risks as they arise. According to all participants, the constant improvement training must evolve in response to the threats faced by the organization, as well as its needs. P3 and P5 identified continuous feedback from the various frequent sessions, while P6 and P4 also identified the inclusion of content updates and the relevance of the training programs.

P6 stated that, “There is a need to collaborate with professional security training business entities to help implement adequate compliance and capacity-building training at all employee grade levels.” The professional training business entities deliver structured and content assessments that utilize evolving and changing risk concepts as they arise, helping employees identify security risk trends and ways to mitigate them across various business departments. The response from the participants confirmed the need for a continuous review and implementation of training programs and development of trainings to different participants within the organization to help align with growing sophistications in cyberattack.

Theme 4: Human Factor in Cybersecurity and Emerging Technologies

Human beings are the bedrock of any compliance strategy implementation and as a result should be given high priority to enable the successful implementation of risk control procedures within an organization. According to P1 and P2, humans are the weakest link, and therefore, there is an adequate need to ensure they are adequately monitored and guided to do the right thing at all times. Employees of organizations, especially non-technical staff, should have a limit on what can be accessed online from the business network. Management should ensure that adequate controls are in place to monitor and check employees' online habits, including what they access and what they should not.

According to P3 and P4, employees should be vigilant about what they do, watch, or download online, as well as monitor external devices to ensure they avoid internal compromise. Employees should be proactive and consider both the short-term and long-

term implications of control failures, and as a result, follow the established rules for all transactions. The continual changes in nature and volume of attacks will also require continual upgrades and training of employees to be updated on the risk trend. According to P4, “Employees must be able to adapt to changes and ensure they comply with the rules and also apply the knowledge gained from training in their daily job functions.” Organizational leaders should also ensure that there is adequate documentation of knowledge and information available for training to help keep new employees up to date, especially in a volatile environment where there is high employee turnover. This theme emphasized the importance of human involvement in ensuring adequate protection against cyberattack.

Theme 5: Key Cybersecurity Threats

The advent of technological innovations worldwide has increased the volume of business and personal transactions conducted online. The increase has also led to increased exposure to cyberthreats and attacks from both insiders and outsiders. For business entities, threats and exposure can cause significant reputational damage and financial losses if not properly managed. It is essential to be aware of the various types of threats that may expose individuals to potential harm, enabling them to protect themselves effectively. According to P1, P2, P3, and P6, social engineering is a significant threat that business entities should be aware of and ensure adequate protection against. Social engineering is a method of obtaining unauthorized sensitive information by manipulating individuals into believing and trusting a source of requests, thereby compromising the organization's security network. Social engineering typically involves

attackers gathering information to identify weaknesses in potential targets. Then they gain the target's trust by posing as a trusted source, before exploiting them. As a result, the victims become bait and compromise their security due to the psychological triggers of urgency in their actions. Different types of social engineering methods include phishing, smishing, vishing, baiting, pretexting, quid pro quo, scareware, and tailgating.

P2 and P4 identified information leakage by employees as a threat to the organization, while P2 identified information leakage by vendors as a risk to the organization. P3 and P5 identified technological vulnerabilities and data privacy issues as threats to Organizations. According to P5, “The Central Bank of Nigeria (CBN) regulatory requirements are cumbersome and sometimes conflicting to follow. They need to be aligned and simplified for easy guidance and compliance.” Overall, if organizations can mitigate social engineering exposures, they will put themselves in a more secure and less risky position against other threats.

Theme 6: Cybersecurity Awareness Strategies

There is growing concern for awareness programs for cybersecurity issues among employees. Employees can achieve awareness through effective communication networks. When identifying communication networks, it is essential to consider the timeliness and ability to verify the effectiveness of the strategies. According to P1, “Organization must foster a culture of accountability that enables employees to take charge of their actions without being forced.” Employees must understand the impact of their actions, which can positively or negatively affect the business's exposure to risk.

From P2's statements, "Business leadership should encourage employees to continue training and be active in protecting the organization."

Any identified threats should be escalated by employees or supervisors and documented adequately for remediation and future reference. According to P2, despite having trust in the data or information received, employees should ensure that they verify all sources of information accurately and thoroughly. P4 commented that, "There is need for organizations to implement a top-down and bottom-up cultural approach to enable employees from all levels of the organization's hierarchy to understand risk and cyberattacks, thereby overcoming their effects." P4 and P5 identified mandatory induction programs as a means for organizations to train their employees adequately. According to P5, "Management should incorporate practical exercises to enable employees to train in real-time scenarios." Real-time practical training will help them understand and be aware of how they can safeguard the organization against future attacks.

Theme 7: Compliance and Regulatory Challenges

The high impact of cyberattacks on both businesses and individuals has necessitated the need for regulatory alignment of processes and the institution of controls with adequate monitoring. According to all participants, financial and budget limits have been a significant hindrance to the proper implementation of controls as the technology world evolves. The continuous exposure of organizations to new threats requires business entities to continually invest in compliance strategies to avoid and protect themselves from cyberattacks. As a result, organizational leadership should provide adequate funding

for business entities and empower the compliance department to employ professionals to help curb exposures to external and internal risks and threats. According to P2, “There is need for Management to provide adequate compensation for compliance team employees to avoid or reduce staff turnover and mobility.”

P1, P3, and P4 identified leadership resistance as a constraint to adequate employee training, thereby increasing the business's exposure to cyberattacks. They recognized the need for management leadership to adopt training and allocate sufficient resources to mitigate exposure to threats and cyberattack. P6 also identified the need for training to be prepared and delivered with role-specific relevance, enabling different departments of the organization to have a better understanding of how their roles can help protect the organization against cyberattacks. P5 also identified the need for employees to be trained by management on the impact of data privacy risks and the importance of protecting customer information against exposure to vulnerable sources. P5 and P6 also identified regulatory complexities from the regulatory body and the need to ensure that the bodies adequately address them. In summary, it is argued that compliance and regulations should help to encourage a safe attitude by employees rather than discourage them.

Theme 8: Return on Investment on Training

The overall purpose of the training program is to equip employees to manage business activities in a manner that minimizes exposure to risks and potential attacks. The adequate and effective implementation of controls will help limit the losses of organizations from both attacks and sanctions by regulatory bodies. To ensure an

acceptable return on investment is achieved by the business, management must equip employees with the skills necessary to protect the business against losses from attacks. According to P1, “The use of information technology to improve operational efficiency will help increase returns on investment.” P2 identified the opportunity for training to empower employees to gain high technical resilience skills against threats and cyberattacks to the business.

In understanding how return on investment is measured, the participants identified financial, operational, and cultural metrics for measurement. According to the participants, returns should not only be considered from an economic perspective but in a broader approach. The wider aspects can contain conditions such as a reduction in incident reports, a decrease in financial losses, an increase in trust, improved efficiency of business operations, fewer sanctions, or a decrease in penalty/fines payment due to non-compliance by regulatory authorities, improved reporting techniques, employee behavior and culture improvement, and adequate safeguards of organizational assets. P3 stated that “the downtime of operations due to technical or human factors will be reduced.” Overall, training has helped reduce exposure to threats and cyberattack, thereby enabling organizations to improve their performance and increase profits.

Connection of the Findings to the Literature Review

The findings of this study confirmed and extended existing knowledge about employee training and cybersecurity compliance, aligning with the frameworks of PMT and TQM. The comparison between the results and previous literature demonstrated that

leadership involvement, training effectiveness, and human factors remain critical determinants of organizational cybersecurity resilience.

The first major theme, leadership involvement, confirmed existing studies emphasizing the role of leadership in shaping cybersecurity culture and employee behavior (Haag et al., 2021; Wong et al., 2022). The participants emphasized that leadership by example, policy enforcement, and resource allocation, motivate employees to adopt compliant behaviors, aligning with PMT's focus on threat and coping appraisal. Compared with earlier research, this project extends knowledge by highlighting that leadership accountability not only influences compliance but also increases employee trust and willingness to engage in training. These insights expand TQM's principle of continuous improvement by integrating cybersecurity culture as a quality management outcome.

The second theme, training effectiveness, methods, and challenges, confirmed prior findings that effective cybersecurity training enhances compliance and behavioral change (Butavicius et al., 2022; Chowdhury et al., 2023). The participants' emphasis on simulation exercises, phishing tests, and post-training assessments validated the argument that experiential learning improves coping efficacy and self-confidence. This project extended the literature by identifying that periodic evaluation and feedback mechanisms are essential for maintaining training relevance, a point not strongly emphasized in prior research. In line with TQM, continuous monitoring of training outcomes was found to strengthen long-term behavioral consistency, demonstrating that training should be adaptive and responsive to emerging cyberthreats.

The third significant theme, customized and continuous training, supports findings from Shaban et al. (2023) and Wilson et al. (2023), who observed that training tailored to specific roles enhances employee awareness. This project offers new insights by linking customised training to employee engagement and departmental collaboration, confirming that a one-size-fits-all approach is inadequate. It further extends PMT by demonstrating that personalized content enhances both perceived severity and response efficacy among employees, thereby strengthening their motivation to adhere to cybersecurity policies.

Findings on human factors also confirmed that employees are both the weakest and strongest links in cybersecurity management (Hughes-Lartey et al., 2021). Participants emphasized the need for continuous behavioral monitoring, guidance, and reinforcement. This aligns with prior literature but extends it by proposing practical strategies such as integrating behavioral analytics and mentorship-based reinforcement. The project confirmed that technical controls alone cannot substitute for consistent behavioral improvement, thus validating the interdependence between human and technological resilience proposed in TQM.

Furthermore, findings on compliance challenges and regulatory alignment confirmed the financial and structural barriers reported by Shaikh and Siponen (2023). However, the project advanced understanding by showing that leadership resistance and inadequate budgeting directly hinder cybersecurity maturity. Addressing these gaps requires leaders to view compliance as both a regulatory and a profitability issue,

consistent with the emerging literature after 2022, which emphasizes cybersecurity governance as a driver of organizational trust.

This project contributes to scholarly conversation by synthesising behavioral, managerial, and systemic insights into a cohesive model of cybersecurity training. It validates PMT's behavioral premise while extending TQM's principles to digital risk management. The integration of continuous, role-based training and a leadership-driven culture thus represents a novel contribution to the discipline. It provides actionable implications for organizational leaders seeking to strengthen cybersecurity compliance.

Connection of the Findings to the Conceptual Framework

This research project was underpinned by two conceptual frameworks: PMT and TQM. The PMT, which was developed by Rogers (1975), explained how individuals respond to perceived threats based on their appraisal of the severity of the danger and their ability to cope with it. TQM, on the other hand, was developed by theorists such as Deming, Juran, and Crosby, and emphasized continuous improvement, employee involvement, and customer satisfaction as key drivers of organizational success. The findings from this project aligned with both frameworks and extend them in meaningful ways.

Theme 1: Leadership Involvement

Leaders who model cybersecurity best practices and enforce compliance foster more motivation for protection among employees leadership involvement is key in influencing employees' threat appraisal and mechanisms to cope. As a result, the project aligned with PMT's emphasis on perceived severity and efficacy. From the TQM

perspective, leadership is central to cultivating and ensuring a culture of quality and safety. The findings highlight the importance of leadership by example, strategic direction, and resource allocation as core principles of TQM.

Theme 2: Training Effectiveness, Methods, and Challenges

TQM considers the improvement in processes through training results based on continuous improvement. There is a need to ensure adequate use of feedback to improve processes and employee commitment to ensure adequate implementation of changes for the success of the business enterprise. All levels of management at the organization should be involved in the improvement process. PMT suggests that practical training helps employees with chances of adequate coping appraisal, increasing their confidence and motivation to act securely and safely, as the use of simulations, phishing tests, and feedback mechanisms supports the PMT conceptual framework.

Theme 3: Customized Training Strategies, Continuous Improvement, and Collaboration

Using tailored, role-specific training and real-world simulations, the perceived self-efficacy and response efficacy of employees improved, reinforcing the agreement with PMT. Van et al (2021) identified increased interest in cybersecurity using video-based and game-based learning methods of training to increase compliance and reducing the cyberattack exposure of businesses. TQM considers developing and improving contents of training, providing regular training updates, and collaborating with external experts and professionals to ensure relevance and effectiveness, thereby aligning with its emphasis on process optimization and stakeholder engagement.

Theme 4: Human Factor in Cybersecurity and Emerging Technologies

Human behavior can be considered as the weakest link in cybersecurity, as acknowledged by PMT. Adequate monitoring, guidance, and education of employees enhance their ability to recognize and respond to threats promptly and effectively. According to Alammar et al (2025), social media plays a significant role in disseminating information to employees. TQM emphasizes employee involvement and empowerment, and the project findings support the need for adequate documentation, knowledge transfer, and continuous training to maintain quality and resilience at all levels of employee hierarchy.

Theme 5: Key Cybersecurity Threats

PMT is important by understanding the various threats experienced by both individuals and businesses. Examples include social engineering that exploits psychological triggers. Enhancing awareness and building coping strategies helps employees resist manipulation more effectively. Sipior et al (2018) identified that ransomware attackers constantly create new variants to bypass any form of intrusion detection or antivirus software that may be created by organizations. TQM contributes by promoting systematic approaches to threat identification and mitigation, including compliance with relevant regulatory standards and process control.

Theme 6: Cybersecurity Awareness Strategies

Organizations need to develop strategies that make employees aware of risks based on threat appraisal and coping efficacy and helps to reduce their impact aligning with PMT. Building a culture of accountability among employees and encouraging

proactive behavior against risks and threats are keys to motivating protective actions.

TQM considers timely feedback, detailed training, and continual improvement, that will help to inform and improve new employee induction programs, practical exercises, and cultural transformation approaches.

Theme 7: Compliance and Regulatory Challenges

PMT supports the need for protective motivation in response to regulatory threats and organizational vulnerabilities. The findings show that financial constraints and leadership resistance hinder compliance efforts, reducing employees' ability to respond effectively. Reeves et al (2021) considered employee disengagement by exhibiting workplace behaviors due to cybersecurity fatigue because of overexposure to trainings. TQM emphasizes the importance of resource allocation, role-specific training, and process alignment with regulatory requirements, thereby highlighting the need for strategic investment by organizational leadership and their commitment to implementation.

Theme 8: Return on Investment on Training

PMT suggested that behavior of employees can help protect the business based on how they perceive a benefit to their actions. The findings demonstrate that training enhances technical resilience, reduces incidents, and improves operational efficiency, thereby validating the motivational aspect of PMT. These actions are expected to increase the business's returns on investment by reducing losses. TQM's broader view of ROI encompasses financial, operational, and cultural metrics, emphasizing the positive results

achieved through training, including improved performance, reduced penalties, and safeguarded organizational assets.

The findings of this project demonstrate a strong alignment with both PMT and TQM. Humaidi et al. (2022) reflected on the need to ensure that cybersecurity protective behavior is constantly reevaluated among employees, thereby reducing or avoiding the impact of attacks on the business. PMT provides insight into individual behavioral responses to cybersecurity threats, while TQM offers a framework for organizational processes, leadership strategies, and continuous improvement. Together, these frameworks support a holistic approach to cybersecurity that integrates on how training can improve human behavior, leadership, risk, compliance, and strategic investment.

Table 3*Thematic Matrix: Cybersecurity Compliance and Training Strategies*

Theme	Participant						Dominant insight
	P1	P2	P3	P4	P5	P6	
Cybersecurity threats	Social engineering, vendor risk	Info leakage, social engineering	Phishing, tech vulnerabilities	Insider threats, API misconfigure	CBN regulations, data privacy	Insider threats, phishing, vendor risk	Human error and external threats are universal concerns.
Training strategies	Workshops, reminders, tailored formats	Spot checks, phishing tests	Onboarding, regular training	Infographics, focus groups	Reward-driven, simulations	Real-world simulations, focus groups	Training must be continuous, engaging, and role-specific.
Effectiveness assessment	Pre-/posttests, behavior tracking	Simulated attacks, penetration tests	Surveys, phishing tests	Click rates, reporting patterns	Incident tracking, financial loss comparison	Click rates, behavior change, incident reports	Simulations and behavioral metrics are key tools.
Leadership's role	Model behavior, reward systems	Sanctions, compliance enforcement	Mandatory participation, follow-up	Executive buy-in, board interest	CISO engagement, management support	Strategic direction, resource allocation	Leadership drives culture, credibility, and resource access.
ROI measurement	Avoided losses, trust, efficiency	Vulnerability reduction	Incident reduction	Fewer fines, less downtime	Loss reduction, improved reporting	Reduced fines, improved behavior	ROI includes financial, operational, and cultural metrics.
Training delivery methods	Mix of in-person/digital	In-person sessions	E-learning and workshops	Infographics, simulations	Self-paced and hands-on	Instructor-led preferred	Blended formats enhance accessibility and retention.
Continuous improvement	AI updates, feedback loops	Quizzes, evolving threats	Feedback, content updates	Threat intelligence, relevance	Roadmap, frequent sessions	Content updates, cross-department alignment	Training must evolve with threats and organizational

Theme	Participant						Dominant insight
	P1	P2	P3	P4	P5	P6	
Human-centric cybersecurity	Accessible content for all staff	Final line of defense	Reporting comfort, proactive staff	Vigilance culture, customer education	Awareness reduces incidents	Behavior change, password hygiene	needs. Humans are the frontline— Training must empower them.
Compliance challenges	Resistance, complexity, budget	Mobility, tech pace	Financial limits, management buy-in	Non-tech engagement; accessibility	Management buy-in, regulatory pressure	Regulatory overlap, resistance to AI	Budget, resistance, and regulation are recurring hurdles.

Note. API = application programming interface; CBN = Central Bank of Nigeria; CISO = chief information security officer; ROI = return on investment.

Business Contributions and Recommendations for Professional Practice

This project contributes significantly to professional practice by offering a dual-theoretical lens using PMT and TQM. Both PMT and TQM enhance understanding and improve cybersecurity compliance within organizations. The findings identified actionable insights on how training can help businesses achieve improved financial and overall business results. The business can benefit from a strategic training development plan that utilizes customized, role-specific training programs incorporating simulations and real-world scenarios. The training will enhance employee preparedness and reduce vulnerability to cyberthreats.

In addition, identifying the important role leadership plays in shaping cybersecurity culture can improve the engagement of leaders in reducing the impact of attacks on the business. Business leaders can model desired behaviors and effective resource allocation, thereby fostering a proactive and compliant workforce. The human-centric cybersecurity strategy helps to ensure that business entities identify employees as both the weakest link and the most robust defense, thereby emphasizing the need for continuous education, monitoring, and support to build resilience. Threat awareness and risk management identify important threats faced by business entities. According to Obadire et al. (2023) social engineering and leakage of data to external parties can be reduced by implementing targeted interventions and the development of policies to reduce the impact of the risks. Ensuring adequate compliance and regulatory alignment is essential for business survival and profitability. The findings of the project show the importance of aligning organizational practices with regulatory requirements, which is

supported by adequate funding and a strong leadership commitment. Return on Investment (ROI) in training is also an aspect of leadership focus. Training programs are meant not only to reduce incidents and improve operational efficiency but also to contribute to cultural transformation and regulatory compliance, offering measurable ROI across financial, operational, and behavioral dimensions.

Based on the business implications outlined above for the project, it is essential to provide recommendations for professional practice. Firstly, business leadership should develop a cybersecurity leadership framework that encourages leaders at all levels to actively participate in cybersecurity initiatives, model best practices, and foster a culture of accountability. Secondly, there should be an implementation of continuous and adaptive training programs. The training of employees should focus on responding to emerging threats, by incorporating timely and effective feedback, tailored to specific roles and departments. Thirdly, human factor controls should be strengthened to introduce policies that limit access based on roles, constant monitoring of online behavior, and promoting vigilance among employees, especially non-technical staff.

Adequate investment in threat intelligence and awareness campaigns can help businesses overcome threats from cyberattack. Regularly updating employees on new threats and providing practical tools to recognize and respond to social engineering and other attack vectors will help reduce threats. There is a need to align compliance strategies with business objectives. This can be achieved by ensuring that compliance efforts are adequately funded, strategically integrated, and supported by leadership to meet regulatory demands and reduce risk exposure. There is also a need to measure and

communicate the ROI of cybersecurity training. Using different variables like operational, financial, and cultural conditions, managers can evaluate the effectiveness and adequacy of training to meet the needs of stakeholders. Partnering with cybersecurity experts and training providers can enhance internal capabilities and stay ahead of evolving threats.

Implications for Social Change

The findings of this project have meaningful implications for social change, particularly in how organizations, individuals, and communities approach cybersecurity awareness, compliance, and resilience through training. By integrating PMT and TQM, the project provides a framework for promoting both behavioral and systemic transformation that extends beyond the workplace. This can result in the promotion of a cybersecurity awareness culture. The project emphasizes the importance of building a culture of accountability and vigilance among employees. The shift in culture can encourage individuals to adopt safer practices online, thereby reducing the impact of the overall vulnerability to cyberattack and threats. Education can also help empower individuals.

Training and awareness programs equip individuals with the experience and skills to recognize and respond to cyberthreats. This knowledge gives informed and proactive actions by employees that are capable of protecting personal and community data and resisting manipulation through social engineering. Ethical leadership and governance can also be encouraged. According to Humaidi et al (2022) the behavior shown by the top management can enlighten junior employees to improve their security culture and help in

practicing good cybersecurity behavior. The findings underscore the pivotal role of leadership in driving compliance and fostering cultural change. Ethical leadership should prioritize cybersecurity and employee well-being to encourage and empower broader influence on governance practices, promoting transparency, accountability, and responsible innovation.

Strengthening institutional trust through improved cybersecurity practices can lead to fewer breaches, reduced financial losses, and enhanced data privacy. According to Badhwar (2021) inadequate security can cause unintended consequences (i.e., cyberattack), therefore organizational leaders should be committed to adopting new technologies and innovative processes to avoid disruption and losses. The improvement in institutional trust should strengthen public trust in institutions, whether businesses, governments, or service providers, and also promote a more secure and stable digital environment. There will also be a reduction in digital inequality. By considering training strategies that are role-specific and inclusive the project supports that cybersecurity education should be accessible to all, including non-technical staff and marginalized groups. The role specific training contributes to reducing digital inequality and ensuring that all members of society can participate safely in the digital economy. Ultimately, by enhancing organizational resilience and safeguarding digital infrastructure, the project contributes to sustainable development and inclusive growth.

Recommendations for Further Research

I recommended that future investigators focus on identifying the impact, if any, that employee age has on the effectiveness of cybersecurity training programs. This may

include the analysis of generational differences in how cybersecurity risks are understood, their participation and reaction to training. According to Redekop (2021) there is evidence showing that younger generations (millennials and Gen Z) prefer technology over their older counterparts. Research on this generational difference would help businesses to develop custom training programs that align with the unique learning styles and familiarity with technology of particular groups. This strategy would enhance employee engagement and training effectiveness, as there will be an increase in the effective implementation of cybersecurity compliance strategies across all age groups.

It is recommended that future studies can be undertaken to increase the range of organizations to represent the different geographical locations. As cyberthreats represent a global phenomenon, it would be a useful topic to examine how different cultures and business contexts have developed their cybersecurity compliance strategies. For example, compliance outcomes may be influenced by regulatory differences, organizational structure, and the employees attitudes towards cybersecurity. Studies in this field would assist companies with more insight into the implications of cultural differences on the behavior and compliance of employees, which ultimately would enable multinational organizations to prepare globally applicable approaches.

The limitation of the present research is that the analysis was carried out from a short-term perspective. In response to this, I recommend that future researchers explore the long-term effects of training on cybersecurity behavior and compliance in workers. Longitudinal research might be conducted on employees over a few years to determine the effectiveness of retaining knowledge following the training session and whether the

knowledge produces lasting behavioral changes in cybersecurity practices. Such studies would prove helpful particularly to the companies that are interested in long-term and sustainable training investment.

I suggest that training in cybersecurity must also be based on future studies about the incorporation of new technologies in the shape of AI, virtual reality, and machine learning. Research on this area may be performed concerning the manner, in which these technologies may be utilized further in order to deliver more animated and interactive training programs to the employees. Using the example, AI can follow the training modules according to the employees' individualities and requirements, reacting to the learning uniqueness of their employees, yet virtual reality can reproduce the situation in real life, providing the employee with recommendation in their response to the cyberthreat. When such technologies get investigated, it would allow companies to better understand cybercriminals by updating their training programs constantly on the new threats.

Possibilities for Addressing Research Limitations

Future researchers could expand the perspective on cybersecurity leadership to a wider geographical representation that entertains the whole of North America, Europe and Asia. This would allow cross-cultural comparisons and more generalized outcome. The sample size might have been extended to enhance the reliability and generalizability of the findings. Further research may be of benefit by enabling the comprehension of the effectiveness of the cybersecurity compliance strategies because more participants will be involved which will represent a range of industries and organizations. The current

research, as mentioned, focuses on short-term outcomes. Longitudinal research designs could prove useful in future studies in order to determine the extent to which cybersecurity training will reduce or sustain long-term behavioral changes in employees and organizational compliance.

Conclusion

In conducting this project, I sought to identify how leaders in cybersecurity can influence their employees to comply, which increases the profitability of the business by mitigating cyberthreats. In this research, the qualitative pragmatic inquiry design was accommodated using semistructured interviews with six cybersecurity leaders. This project was conducted to gain insights on effective strategies of improving adherence to cybersecurity measures in employees. The interviews were transcribed and later thematically analysed in line with the method introduced by Braun and Clarke. The data was collected among the professionals having an experienced background connected to the organization of cybersecurity compliance. This methodology process also allowed exploration that could at best be considered as exploration of real-life practices and insights that could provide very useful data to answer the research question. The level of accuracy and trustable reliability of the data collected was achieved by using member checking.

The findings of this project offer several valuable suggestions and strategies that may assist business leaders in improving the commitment levels among workers in terms of cybersecurity. First, the role of leadership has become one of the most important themes. When leaders set an example by portraying their preferred behaviors and

showing a personal interest in cybersecurity, they encouraged a compliance culture within their respective organizations. The engagement of the leadership played a vital role in encouraging employees to participate in cybersecurity training and follow the best practices. The outcome was in line with PMT because the leaders assisted the employees in evaluating the perceived seriousness and effectiveness of security threats prompting them to engage in protection behaviours.

Another important finding was the effectiveness of training. The findings of the current analysis further revealed that training programs should be implemented on a continuous basis to deal with the ever-evolving cybersecurity risks. The participants mutually pointed out that real-life simulation and role-specific training are necessary ingredients of training to make it involve and impactful. Training with conventional training that comprised within the lectures was ineffective compared with interactive training with phishing test and simulation attacks training. This illustrates the PMT framework due to the increase of the self-efficacy of employees to respond to threats.

The research also revealed that organizational leaders should create a culture of accountability whereby the organizational employees understand the impact of their behaviours on the organizational cybersecurity posture. This training activity should also focus on skill development and behavior transformation among individuals in order to reduce noncompliance. Leadership is a key factor in developing this accountability culture. The implication of this project was that it required continuous monitoring and measurement of the effectiveness of training and the role-specific training, this assists within meeting the individual needs of various departments within an organization. As a

means of improving and maintaining high rates of cybersecurity compliance, which subsequently advances the business resilience and profitability, the given study outlines the importance of strong leadership commitment, the feeling of responsibility among its staff, and adaptable training plans.

References

- Abimbola, B. O., Oyatoye, E. O., & Oyenuga, O. G. (2020). Total quality management, employee commitment, and competitive advantage in Nigerian tertiary institutions. A study of the University of Lagos. *International Journal of Production Management and Engineering*, 8(2), 87–98.
<https://doi.org/10.4995/ijpme.2020.12961>
- Adler, R. H. (2022). Trustworthiness in qualitative research. *Journal of Human Lactation*, 38(4), 598–602. <https://doi.org/10.1177/08903344221116620>
- Ahmed, S. K. (2024). The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, 2, Article 100051.
<https://doi.org/10.1016/j.glmedi.2024.100051>
- Alammar, L. K. A., Almutairi, G. K. B., Suwaylih, Y. O. A., Alotaibi, N. S. M., Alahmari, R. M. A., & Fiala, L. (2025). Barriers and enabling factors for human papilloma virus vaccination among Saudi parents. *European Journal of Theoretical and Applied Sciences*, 3(3), 266–278.
[https://doi.org/10.59324/ejtas.2025.3\(3\).23](https://doi.org/10.59324/ejtas.2025.3(3).23)
- Alawag, A. M., Alaloul, W. S., Liew, M. S., Baarimah, A. O., Musarat, M. A., & Al-Mekhlafi, A.-B. A. (2023). The role of the total quality management (TQM) drivers in overcoming the challenges of implementing TQM in industrialized building system (IBS) projects in Malaysia: Experts' perspectives. *Sustainability*, 15(8), Article 6607.
<https://doi.org/10.3390/su15086607>

- Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, 11(3), Article 73. <https://doi.org/10.3390/fi11030073>
- Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, 15(12), Article 2175. <https://doi.org/10.3390/sym15122175>
- Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, 129, Article 103208. <https://doi.org/10.1016/j.cose.2023.103208>
- Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behavior. *Personal and Ubiquitous Computing*, 25(5), 829–841. <https://doi.org/10.1007/s00779-021-01551-2>
- Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. *PeerJ Computer Science*, 8, Article e938. <https://doi.org/10.7717/peerj-cs.938>
- Badhwar, R. (2021). *The CISO's next frontier: AI, post-quantum cryptography and advanced security paradigms*. Springer. <https://doi.org/10.1007/978-3-030-75354-2>
- Baldissone, G., Comberti, L., Bosca, S., & Murè, S. (2019). The analysis and management of unsafe acts and unsafe conditions. Data collection and analysis. *Safety Science*, 119, 240–251. <https://doi.org/10.1016/j.ssci.2018.10.006>

- Bekkers, L., van't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security, 127*, Article 103099. <https://doi.org/10.1016/j.cose.2023.103099>
- Blanuša, J., Barzut, V., & Knežević, J. (2021). Intolerance of uncertainty and fear of COVID-19 moderating role in the relationship between job insecurity and work-related distress in the Republic of Serbia. *Frontiers in Psychology, 12*, Article 647972. <https://doi.org/10.3389/fpsyg.2021.647972>
- Braun, V., & Clark, V. (2019). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health, 13*(2), 201–216. <https://doi.org/10.1080/2159676X.2019.1704846>
- Braun, V., & Clark, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher. *International Journal of Transgender Health, 24*(1), 1–6. <https://doi.org/10.1080/26895269.2022.2129597>
- Bunn, M. (2023). Insider threats to nuclear security. In *the oxford handbook of nuclear security*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192847935.013.9>
- Butavicius, M., Taibb, R., & Hanb, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of

phishing emails. *Computers & Security* 123(1), Article 102937,

<https://doi.org/10.1016/j.cose.2022.102937>

Chapman, P. (2020). Are your IT staffs ready for the pandemic-driven insider

threat? *Network Security*, 2020(4). [https://doi.org/10.1016/S1353-4858\(20\)30042-](https://doi.org/10.1016/S1353-4858(20)30042-8)

[8](https://doi.org/10.1016/S1353-4858(20)30042-8)

Chen, H., Li, Y., Chen, L., & Yin, J. (2021). Understanding employees' adoption of the

bring your own device (BYOD): the roles of information security-related conflict and fatigue. *Journal of Enterprise Information Management*, 34(3), 770–792.

<https://doi.org/10.1108/JEIM-10-2019-0318>

Chowdhury, N., & Gkioulos, V. (2023). A personalized learning theory-based cyber-

security training exercise. *International Journal of Information Security*. 22,

1531–1546. <https://doi.org/10.1007/s10207-023-00704-z>

Clarke, B., Alley, L., Ghai, S., Flake, J. K., Rohrer, J. M., Simmons, J. P., & Vazire, S.

(2023). Looking our limitations in the eye: A call for more thorough and honest reporting of study limitations. *Social and Personality Psychology Compass*, 18(7),

Article e12979. <https://doi.org/10.1111/spc3.12979>

Clifton, A. (2024). Strategies for insider threat mitigation and detection.

<https://scholarworks.waldenu.edu/dissertations/15446>

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0:

A structured classification of critical assets and business impacts. *Computers in*

industry, 114(1), Article 103165. <https://doi.org/10.1016/j.compind.2019.103165>

- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, 47, 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*, 27, 4729–4752. <https://doi.org/10.1007/s10639-021-10806-7>
- D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43–69. <https://doi.org/10.1111/isj.12173>
- Dearden, T. E., Parti, K., Hawdon, J., Gainey, R., Vandecar-Burdin, T., & Albanese, J. (2023). Differentiating insider and outsider cyberattack on businesses. *American Journal of Criminal Justice*, 48, 871–886. <https://doi.org/10.1007/s12103-023-09727-7>
- Downing, S. T., Mccarty, R. J., Guastello, A. D., Cooke, D. L., & Mcnamara, J. P. (2023). Assessing the predictors of adaptive and maladaptive Covid-19 preventive behaviors: an application of protection motivation theory. *Psychology, Health & Medicine*, 28(2), 460-474. <https://doi.org/10.1080/13548506.2022.2093925>
- Drisko, J. W. (2024). Transferability and generalization in qualitative research. *Research on Social Work Practice*, 35(1). <https://doi.org/10.1177/10497315241256560>

- Fornell, C., Morgeson, F. V., Hult, G. T. M., & VanAmburg, D. (2020). *The reign of the customer: Customer-centric approaches to improving satisfaction*. Palgrave Macmillan Cham. <https://doi.org/10.1007/978-3-030-13562-1>
- Fu, X., Kong, L., Tang, T., & Yan, X. (2020). Insider trading and shareholder investment horizons. *Journal of Corporate Finance*, 62, Article 101508. <https://doi.org/10.1016/j.jcorpfin.2019.101508>
- Fuchs, K. (2023). A systematic guide for conducting thematic analysis in qualitative tourism research. *Journal of Environmental Management and Tourism (JEMT)*, XIV(6(70)), 2696–2703. <https://www.ceeol.com/search/article-detail?id=1193994>
- 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>
- Hammoumi, A. E., Nabil, S., Mounir G., Meryem, A., & Abdelaziz, B. (2024). The adoption of a qualitative approach in management science: An Exploratory Survey on the Effects of Big Data on the Performance of Companies . *Applying Qualitative Research Methods to Management Science*, IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-5543-5.ch011>
- Hansen, M. F., Sørensen, P. K., Sørensen, A. E., & Krogfelt, K. A. (2023). Can protection motivation theory predict protective behavior against ticks? *BMC Public Health*, 23(1), 1–11. <https://doi.org/10.1186/s12889-023-16125-5>
- Haq, Z. U., Rasheed, R., Rashid, A., & Akhter, S. (2023). Criteria for assessing and

ensuring the trustworthiness in qualitative research. *International Journal of Business Reflections*, 4(2). <https://doi.org/10.56249/ijbr.03.01.44>

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cybersecurity readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58(1), Article 102726.

<https://doi.org/10.1016/j.jisa.2020.102726>

Hina, S., & Dominic, P. D. (2020). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, 60(3), 201–211. <https://doi.org/10.1080/08874417.2018.1432996>

Hodgins, M., MacCurtain, S., & Mannix-McNamara, P. (2020). Power and inaction: why organisations fail to address workplace bullying. *International Journal of Workplace Health Management*, 13(3), 265–290. <https://doi/10.1108/IJWHM-10-2019-0125/full/html>

Hubbard, T., Klimavicz, J. F., Wong, S., & Steinhoff, J. C. (2021). Zero trust in a virtual cybersecurity world. *The Journal of Government Financial Management*, 70(2), 12–19. <https://www.proquest.com/openview/30c22f6430bce1b543c850b3963373b7/1?pq-origsite=gscholar&cbl=26015>

Hughes-Lartey, K., Li, M., Botchey, F., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *ScienceDirect*. <https://doi.org/10.1016/j.heliyon.2021.e06522>

- Huising, R., & Silbey, S. S. (2021). Accountability infrastructures: Pragmatic compliance inside organizations. *Regulation & Governance*, *15*(S1), S40–S62.
<https://doi.org/10.1111/rego.12419>
- Humaidi, N., & Abdallah Alghazo, S. H. (2022). Procedural information security countermeasure awareness and cybersecurity protection motivation in enhancing employee's cybersecurity protective behavior. 2022 10th International Symposium on Digital Forensics and Security (ISDFS), 1–10. Istanbul, Turkey.
<https://doi.org/10.1109/ISDFS55398.2022.9800834>
- Jaeger, L., Eckhardt, A., & Kroenung, J. (2021). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. *Information & Management*, *58*(3), Article 103318.
<https://doi.org/10.1016/j.im.2020.103318>
- Jeong, M., & Zo, H. (2021). Preventing insider threats to enhance organisational security: The role of opportunity-reducing techniques. *Telematics and Informatics*, *63*, Article 101670. <https://doi.org/10.1016/j.tele.2021.101670>
- Josephson, A., & Smale, M. (2020). What do you mean by “informed consent”? Ethics in economic development research. *Applied Economic Perspectives and Policy*, *43*(4), 1305–1329. <https://doi.org/10.1002/aepp.13112>
- Katou, A. A., Budhwar, P. S., & Patel, C. (2020). Idiosyncratic deals in less competitive labor markets: testing career i-deals in the Greek context of high uncertainties. *International HRM in an Uncertain World*. *32*(17), 3748–3775.
<https://doi.org/10.1080/09585192.2020.1759672>

- Katsantonis, M. N., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security*, 22, 1005–1027. <https://doi.org/10.1007/s10207-023-00680-4>
- Khan, H., & Sukhotu, V. (2020). Influence of media exposure and corporate social responsibility compliance on customer perception: The moderating role of Firm's reputation risk. *Corporate Social Responsibility and Environmental Management*, 27(5), 2107–2121. <https://doi.org/10.1002/csr.1951>
- Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation-based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, 125, Article 103049. <https://doi.org/10.1016/j.cose.2022.103049>
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employee's information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106, Article 102267. <https://doi.org/10.1016/j.cose.2021.102267>
- Khatib, R., & Barki, H. (2020). An activity theory approach to information security non-compliance. *Information & Computer Security*, 28(4), 485-501. <https://doi.org/10.1108/ICS-11-2018-0128>
- Koohang, A., Nord, J. H., Sandoval, Z. V., & Paliszkievicz, J. (2021). Reliability, validity, and strength of a unified model for information security policy

compliance. *Journal of Computer Information Systems*, 61(2), 99–107.

<https://doi.org/10.1080/08874417.2020.1779151>

Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022). What changed in the cyber-security after COVID-19?. *Computers & security*, 120, Article 102821.

<https://doi.org/10.1016/j.cose.2022.102821>

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

Lee, H. (2021). Changes in workplace practices during the COVID-19 pandemic: the roles of emotion, psychological safety and organisation support. *Journal of Organizational Effectiveness: People and Performance*, 8(1), 97–128.

<https://doi.org/10.1108/JOEPP-06-2020-0104>

Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting instant messaging phishing attacks: the role of self-efficacy and the mediating effect of attitude towards online sharing of personal information. *International Journal of Environmental Research and Public Health*, 20(4), Article 3514.

<https://doi.org/10.3390/ijerph20043514>

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24.

<https://doi.org/10.1016/j.ijinfomgt.2018.10.017>

- Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, 5(1), Article 100165. <https://doi.org/10.1016/j.chbr.2021.100165>
- Lim, W. M. (2024). What is qualitative research? An overview and guidelines. *Australasian Marketing Journal (AMJ)*, 33(2), <https://doi.org/10.1177/14413582241264619>
- Liu, C., Liu, Y., Wang, C. & Wang, H. (2021, June 11-13). Exploring the impact of information security climate and information security training on cybersecurity behavior: Based on protection motivation theory (PMT). 6th International Symposium on Computer and Information Processing Technology (ISCIPT). Changsha, China. <https://doi.org/10.1109/ISCIPT53667.2021.00168>
- Locke, K., Feldman, M., & Golden-Biddle, K. (2020). Coding practices and iterativity: beyond templates for analyzing qualitative data. *Organizational Research Methods*, 25(2), 262–284. <https://doi.org/10.1177/1094428120948600>
- Loi, M., Gordijn, B., & Christen, M. (2020). The Ethics of Cybersecurity. *The International Library of Ethics, Law and Technology*, Springer., <https://library.oapen.org/bitstream/handle/20.500.12657/22489/1/1007696.pdf#page=88>
- Malatji, M., Marnewick, A. L. & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security*, 30(2), 255–279. <https://doi.org/10.1108/ICS-06-2021-0091>

- Marina, H., & Simone, D. (2023). Personal protective behaviors in response to COVID-19: a longitudinal application of protection motivation theory. *Frontiers in Psychology, 14*. Article 1195607. <https://doi.org/10.3389/fpsyg.2023.1195607>
- McDowell, I. (2023). *Theoretical models of health behavior*. Springer Cham. https://doi.org/10.1007/978-3-031-28986-6_6
- McIlwraith, A. (2021). *Information security and employee behavior: how to reduce risk through employee education, training and awareness*. Routledge. <https://doi.org/10.4324/9780429281785>
- Montasari, R. (2024). *Cyberspace, cyberterrorism and international security in the fourth industrial revolution: threats, assessment and responses*. Springer Cham. <https://doi.org/10.1007/978-3-031-50454-9>
- Moody, G. D., Siponen, M., & Pahlila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1). 285–A22. <https://doi.org/10.25300/MISQ/2018/13853>
- Mou, J., Cohen, J. F., Bhattacharjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems, 23*(1), 196–236. <https://doi.org/10.17705/1jais.00723>
- Muzari, T., Shava, G. N., & Shonhiwa, S. (2022). *Qualitative research paradigm, a key research design for educational researchers, processes and procedures: A theoretical overview*. 3(1). [https://indianapublications.com/articles/IJHSS_3\(1\)_14-](https://indianapublications.com/articles/IJHSS_3(1)_14-)

[20_61f38990115064.95135470.pdf](#)

Ncubukezi, T. (2022, March). Human errors: A cybersecurity concern and the weakest link to small businesses. *Proceedings of the 17th International Conference on Information Warfare and Security*, 17(1). New York, USA.

<https://doi.org/10.34190/iccws.17.1.51>

Nweke, L., Bokolo, A., Mba, G., & Nwigwe, E. (2022) Investigating the effectiveness of a hyflex cyber security training in a developing country: A case study.

In Education and Information Technologies. 27. 10107–10133.

<https://doi.org/10.1007/s10639-022-11038-z>

Obadire, A. M., Moyo, V., & Munzhelele N.F. (2023). An empirical analysis of the dynamics influencing bank capital structure in Africa. *International Journal of Financial Studies*, 11(4), 127.

<https://doi.org/10.3390/ijfs11040127>

Padayachee, K. (2022). Understanding the effects of situational crime prevention and personality factors on insider compliance. *Journal of Information Security and Applications*, 70, Article 103338. <https://doi.org/10.1016/j.jisa.2022.103338>

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, 13(1), 103-128. <https://doi.org/10.1108/JGOSS-05-2019-0042>

[0042](#)

Pietrzykowski, T., & Smilowska, K. (2021). The reality of informed consent: empirical studies on patient comprehension—systematic review. *Trials*, 22(57).

<https://link.springer.com/article/10.1186/s13063-020-04969-w>

- Ramanadhan, S., Revette, A. C., Lee, R. M., & Aveling, E. L. (2021). Pragmatic approaches to analyzing qualitative data for implementation science: an introduction. *Implementation Science Communications*, 2(1).
<https://implementationsciencecomms.biomedcentral.com/articles/10.1186/s43058-021-00174-1>
- Rana, S., & Alhamdani, W. (2021) Exploring the need to study the efficacy of VR training compared to traditional cybersecurity training. *International Journal of Computing Information Engineering*. 15(1). 10–17.
<https://publications.waset.org/10011723.pdf>
- Ray, J. V., Baker, T., & Caudy, M. S. (2020). Revisiting the generality of rational choice theory: Evidence for general patterns but differential effects across varying levels of psychopathy. *Journal of Criminal Justice*, 66, Article 101654.
<https://doi.org/10.1016/j.jcrimjus.2019.101654>
- Redekop, B. D. (2021). IT security training and awareness in the multigenerational workplace. *International Journal of Information Security & Cybercrime*, 10(2), 9–15. <https://doi.org/10.19107/ijisc.2021.02.01>
- Reeves, A, Calic, D., & Delfabbro, P (2021). Get a red-hot poker and open up my eyes, it's so boring"1: Employee perceptions of cybersecurity training. *Computers & Security*, 106(1), Article 102281. <https://doi.org/10.1016/j.cose.2021.102281>
- Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *Sage Publications*.
<https://doi.org/10.1177/21582440211000049>

- Reeves, A., Parsons, K., & Calic, D. (2020). Whose risk is it anyway: How do risk perception and organisational commitment affect employee information security awareness. In *International Conference on Human-Computer Interaction*, 12210(1), 232-249. Cham: Springer International Publishing.
https://doi.org/10.1007/978-3-030-50309-3_16
- Robinson, R. S. (2023). Purposive Sampling. *Springer EBooks*, 5645–5647.
https://doi.org/10.1007/978-3-031-17299-1_2337
- 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>
- Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, 97, 587-597. <https://doi.org/10.1016/j.future.2019.03.024>
- Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organisations and critical businesses. *Electronics*, 9(9), 1460. <https://doi.org/10.3390/electronics9091460>
- Schneider, M., & Rahman, S. (2021, December 15-18) Identifying protection motivation theory factors that influence smartphone security measures. 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA. .
<https://doi.org/10.1109/BigData52589.2021.9671882>

- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security, 124*, Article 102974.
<https://doi.org/10.1016/j.cose.2022.102974>
- Shapira, R. (2022). The Challenge of Holding Big Business Accountable. *Cardozo L. Rev., 44*(1), 203.
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/cdozo44&div=8&id=&page=>
- Sipior, J. C., Bierstaker, J., Borchardt, P., & Ward, B. T. (2018). A Ransomware Case for Use in the Classroom. *Communications of the Association for Information Systems, 43*, Article 32. <https://doi.org/10.17705/1CAIS.04332>
- Soltani, E., & Wilkinson, A. (2020). TQM and performance appraisal: complementary or incompatible? *European Management Review, 17*(1), 57–82.
<https://doi.org/10.1111/emre.12317>
- Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management, 58*, Article 102298.
<https://doi.org/10.1016/j.ijinfomgt.2020.102298>
- Subedi, K. R. (2021, December 1). *Determining the Sample in Qualitative Research*. ERIC. <https://files.eric.ed.gov/fulltext/ED618228.pdf>
- Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber-information security compliance and violation behavior in

organisations: A systematic review. *Social Sciences*, 11(9), 386.

<https://doi.org/10.3390/socsci11090386>

Taquette, S. R., & Souza, L. M. B. (2022). Ethical dilemmas in qualitative research: a critical literature review. *International Journal of Qualitative Methods*, 21(21), 1–15. <https://doi.org/10.1177/16094069221078731>

Tushar, S. D. (2025). 67% of Organizations faces cyber-attack in the past 12 months – New Report. <https://cybersecuritynews.com/67-of-organizations-faces-cyber-attack/>

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. *Computers & Security*, 109, Article 102387. <https://doi.org/10.1016/j.cose.2021.102387>

Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management*, 57(4), Article 103212. <https://doi.org/10.1016/j.im.2019.103212>

Van Steen, T., & Deeleman, J. R. (2021). Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, and Social Networking*, 24(9), 593–598. <https://www.liebertpub.com/doi/10.1089/cyber.2020.0526>

Walls, R., Nageswaran, P., Cowell, A., Sehgal, T., White, T., McVeigh, J., Staykov, S., Bassett, P., Mitelpunkt, D., & Sam, A.H. (2024). Virtual reality as an engaging and enjoyable method for delivering emergency clinical simulation training: a

- prospective, interventional study of medical undergraduates. *BMC medicine*, 22, Article 222. <https://doi.org/10.1186/s12916-024-03433-9>
- Wang, X., Wang, C., Yi, T., & Li, W. (2022). Understanding the deterrence effect of punishment for marine information security policies non-compliance. *Journal of Ocean Engineering and Science*. 9(1), 9–12
<https://doi.org/10.1016/j.joes.2022.06.001>
- Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, 40(9), 1119–1131.
<https://doi.org/10.1080/01639625.2018.1461786>
- Wilson, L. W., Alvin, C. M. L., & Yue, W. T. (2023). Where is it in information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quarterly*. 47 (1), 317–342. <https://doi.org/10.25300/MISQ/2022/15713>
- Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66, Article 102520. <https://doi.org/10.1016/j.ijinfomgt.2022.102520>
- Yob, I. M. (2022). *For Profit and for Good*. Ethics International Press Limited.
- Zuwita, R. M., & Rahmatullah, B. (2021). Relationship between PMT appraisals and Security Practice: Analysis of prevention of insider threat in organization success factor. *Ilkogretim Online*, 20(4). <https://doi:10.17051/ilkonline.2021.04.123>

Appendix A: Interview Protocol

1. Communicate with participants to obtain their consent to participate in the interview.
2. Communicate with participants to confirm time and date of availability for interview
3. Create a Zoom meeting link and send to each participant after Step 2.
4. The interview duration will be 30 to 60 min
5. At the beginning of the interview, I verbally requested the participant's permission to consent or reject their agreement to record the interview session for transcription.
6. After accepting the interviewee consent, I thanked them and began the interview session.
7. There were 10 questions for the interview, and they were asked each participant in same order for easy collation and review after the interview
8. After the interview was concluded, I thanked each participant and informed them that I will send the interview transcript to them for their review and approval before conclusion for use in the project.
9. The transcribed interview was sent to each participant for review
10. A follow up member checking interview was conducted to confirm interview transcript and acceptance of the transcript.

Appendix B: Interview Questions

The interview questions are as follows:

1. What are the key cybersecurity compliance threats your organization currently faces?
2. What strategies do you use to foster a culture of cybersecurity awareness and accountability to improve profitability?
3. How do you assess the effectiveness of cybersecurity training programs in reducing compliance risks?
4. What role does leadership communication play in reinforcing cybersecurity training outcomes?
5. How do you measure the return on investment (ROI) of cybersecurity training initiatives?
6. What challenges do you encounter when trying to align training programs with compliance goals?
7. What training delivery methods (e.g., e-learning, in-person, simulations) do you find most effective in cybersecurity compliance and why?
8. How do you ensure continuous improvement in cybersecurity training content and delivery?
9. In your opinion, what are the most important elements of successful cybersecurity training?
10. Is there anything else you'd like to share on this topic?