Tampere University of Applied Sciences

Cybersecurity in Bank: A Case on Employee Engagement and Responsibility for a Secure Digital Environment (SDE) in the Selected Branch

Md Tareq Hasan

MASTER'S THESIS
November 2023

International Business Management

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
International Business Management

MD TAREQ HASAN:
Cybersecurity in Bank: A Case on Employee Engagement and Responsibility for a Secure Digital Environment (SDE) in the Selected Branch

Master's thesis 86 pages, appendix 3 pages
November 2023

With the escalation of digital interconnectedness, cybersecurity is at the core of many sectors, including banking. Ensuring a Secure Digital Environment (SDE) requires not just robust technology but also engaged and responsible employees. This study explores employee engagement and responsibility in the context of cybersecurity within the Pubali Bank Limited, Nandina Branch.

A quantitative research approach is used for this study and a linear regression model is applied to understand the relationship between employee engagement and responsibility in cybersecurity and the independent variables of organizational cybersecurity policy rating, the extent of organizational culture promoting responsibility, and the quality of training. The survey questionnaires are utilized to gather data from the branch's employees. The findings provide insights into how these factors influence employee engagement and responsibility towards cybersecurity, emphasizing the importance of cultivating a cybersecurity culture within the organization.

The study provides recommendations to improve organizational digital environments and business sustainability. Additionally, it suggests potential areas for future research in the same field. This research contributes to a broader comprehension of cybersecurity engagement and responsibility, particularly emphasizing the essential human aspect in establishing an effective secure digital environment (SDE).

Keywords: Cybersecurity, Engagement and Responsibility, Organization, and Secure Digital Environment (SDE)

Contents

ABBREVIATIONS AND TERMS

$(IC)^3$ – Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity

ANOVA – Analysis of Variance

APTs – Advanced Persistent Threats

ATM – Automated Teller Machine

BB – Bangladesh Bank (Central Bank of Bangladesh)

CEA – Cybersecurity Enhancement Act

CID – Criminal Investigation Department

CISA – Cybersecurity & Infrastructure Security Agency

DB – Detective Branch

FBI – Federal Bureau of Investigation

FISMA – Federal Information Security Modernization Act

IC3 – Internet Crime Complaint Center (IC3)

IEC – International Electrotechnical Commission

IoT – Internet of Things

ISO – International Organization for Standardization

NIST – National Institute of Standards and Technology

NIST – National Institute of Standards and Technology

PCI DSS – Payment Card Industry Data Security Standard

RMSE – Root Mean Square Error

SDE – Secure Digital Environment

SDT – Self-Determination Theory

SWIFT – Society for Worldwide Interbank Financial Telecommunication

TAM – Technology Acceptance Model

1. INTRODUCTION

Cybersecurity is a critical concern for banks in the digital age. Given the increasing prevalence of cyberattacks and the extensive use of technology in banking operations, banks must prioritize cybersecurity measures to ensure the security of customer data and the integrity of their systems (Johri & Kumar, 2023). Furthermore, federal regulations require banks to maintain and upgrade security measures regularly, such as virus controls, password protection, intrusion detection, and technical system updates. The banking sector heavily relies on digital platforms for its day-to-day operations, faces an increased risk of cyber threats. This shift to a more digital landscape has necessitated an elevated focus on cybersecurity, especially in financial institutions like banks where the security of customer data is paramount (Bryant, Moshirian, & Wolfe, 2018). Cybersecurity management is no longer a task solely for the IT department; it is a shared responsibility that involves every employee in the organization, from top-level management to the front desk. This has led to a fundamental transformation of the roles and responsibilities within organizations to include employee engagement in ensuring a secure digital environment (SDE).

According to the internet crime report 2022 of FBI, in 2022, the IC3 experienced a total of 800,944 complaints, marking a 5% reduction from the previous year, 2021 globally. Despite the decrease in complaints, the potential cumulative loss increased from $6.9 billion in 2021 to over $10.2 billion in 2022 which has been shown in Figure 01.

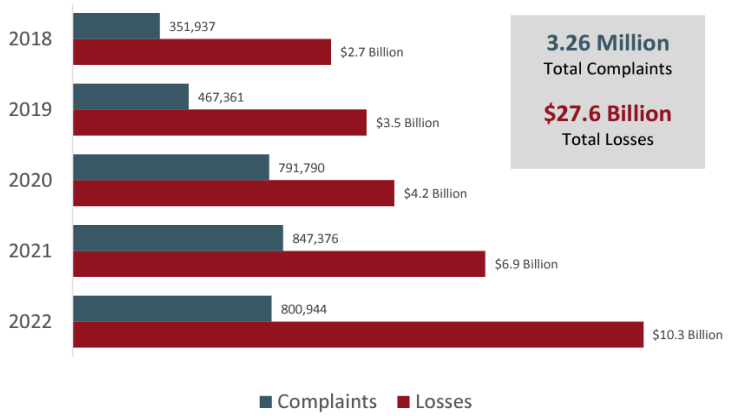

Figure 01: Complaints and Losses over the last 5 years (FBI, 2022)

In 2016, the Bangladesh Bank (BB) suffered a breach leading to a loss of $81 million, considered one of the largest bank robberies ever, and attributed to nation-state hackers. The attackers initiated sending malware-laden emails to bank employees. Once opened, these emails allowed the hackers access to the bank's systems to break the SWIFT network system of BB (The Daily Star , 2016). Later on, in 2019, Dutch Bangla Bank's (local bank) automated teller machines (ATMs) were hacked by an international hacker group. They used cloned cards, which are plastic readable cards capable of taking control over the machines, to steal from nine of the bank's ATMs. Around 1.6 million in local currency was stolen across different areas of the capital, and investigators suspect that other private banks might have been similarly affected. The Cybercrime unit of Counter Terrorism and Transnational Crime (CTTC), DB, and CID of police investigated the cases and identified a lack of cybersecurity within the banks as a contributing factor to the thefts (Staff Correspondent, 2019).

The importance of a secure digital environment (SDE) for banks cannot be overstated. As data breaches become more commonplace, the consequences for banks can be catastrophic, ranging from financial losses to reputational damage that can deter potential customers (Johnson, 2020). Notably, it's not just the technological defenses that determine a bank's cybersecurity posture but also the human element: the employees.

Employee engagement and responsibility play a pivotal role in establishing and maintaining a robust SDE. Engaged employees, who are informed and proactive about security practices, act as the first line of defense against cyber threats. Their actions, or lack thereof, can either prevent or inadvertently facilitate a cyber-attack. For instance, a report by Allen, Green, & Wilson (2018) highlighted that nearly 90% of cyber breaches were due to human error or behavior, emphasizing the critical role employees play in cybersecurity.

Employee engagement, responsibility, and cybersecurity are interconnected. Engaged employees are more likely to adhere to cybersecurity policies, report suspicious activities, and adopt a security-first mindset, thereby bolstering the organization's

cybersecurity defenses (Turner, Jenkins, & Cross, 2021). This heightened sense of responsibility stems from various factors including an organization's cybersecurity policy, its culture of promoting responsibility, and the quality of cybersecurity training provided (Barker & Roberts, 2017).

The objective of this thesis is to explore the dynamic relationship between the employee engagement and responsibility toward cybersecurity and organizational cybersecurity policy, organizational culture, and training to ensure a secure digital environment (SDE) within the Pubali Bank Limited, Nandina Branch. This research aims to contribute to the existing body of knowledge by providing valuable insights into the importance of employee engagement and responsibility in cybersecurity practices within the banks. The findings help identify improvement areas, provide recommendations for enhancing employee engagement and responsibility, and support the banks in developing effective cybersecurity strategies and measures that align with their business sustainability objectives. The implications of this research are extensive and relevant, not only to the case company but also to the wider banking sector, which shares similar challenges and opportunities in the digital age.

1.1 Background

In the contemporary era of digitalization, the banking sector is at the forefront of adopting technological innovations to facilitate transactions and improve customer experience (Khan, 2019). With the extensive utilization of online platforms, mobile banking, and automated systems, banks are increasingly exposed to cybersecurity threats that jeopardize the privacy and security of customer data and financial assets (Sullivan & Burger, 2020).

The cybersecurity landscape has drastically changed over the last decade, with cybercriminals becoming more sophisticated and employing a wide array of tactics to target banking institutions (Cheng, Li, & Yu, 2022). The financial implications of data breaches have reached alarming proportions, with the global average cost of a data breach in 2021 estimated at $4.24 million, marking a significant increase from the previous years (IBM, 2021). In response, governments and regulatory bodies have

implemented stringent regulations to safeguard the integrity and confidentiality of financial data (Gordon, Loeb, & Zhou, 2017).

While technological defenses form the foundation of cybersecurity, human factors play a pivotal role in the security framework. Employee engagement and responsibility in cybersecurity practices are essential to fortifying the security posture of financial institutions (Parsons et al., 2017). Employees act as the first line of defense against potential cyber threats and their understanding, commitment, and adherence to security protocols can significantly reduce the likelihood of successful attacks (Kaspersky, 2019).

Moreover, research by KnowBe4 (2020) indicates that human error is a leading cause of security incidents, highlighting the urgent need for effective engagement, training, and awareness programs. Organizational culture, policy enforcement, and continuous education are key to fostering a security-aware workforce (Soomro, Shah, & Ahmed, 2016). Investment in training and the integration of cybersecurity into the organizational culture has shown to improve employee engagement and reduce risks (Barker & Roberts, 2017).

In light of the above, this study aims to investigate the relationship between the employee engagement and responsibility towards cybersecurity and the organizational policy, culture and training to ensure a secure digital environment (SDE) within the context of the Pubali Bank Limited, Nandina Branch. The emphasis on employee engagement and responsibility in cybersecurity resonates with the global trend towards a comprehensive security approach that includes both technological and human dimensions.

1.2 Objective

The objective of this thesis is to explore the connection between employee engagement and responsibility towards cybersecurity, and how it relates to organizational cybersecurity policies, culture, and training, specifically within the chosen branch. The specific research objective is as follows:

- To identify the key factors influencing employee engagement and responsibility in the context of cybersecurity.

This research examines how employees engage with and take responsibility for cybersecurity, identifies the main factors that influence these areas, and assesses their impact on the overall secure digital environment (SDE). Additionally, it suggests strategies and measures that banks can implement to improve employee commitment and accountability for maintaining an SDE, all with an emphasis on sustaining the business.

1.3 Research Questions

To achieve the stated research objectives, this study is guided by a focused research question 'What are the key factors influencing employee engagement and responsibility in the context of cybersecurity in the branch?' along with three related sub-questions such as How does an employee rate the organization's overall cybersecurity policy, how much does the bank's culture encourage employees to be responsible for cybersecurity, and how does an employee rate the organizational training on cybersecurity practices and responsibilities. A table is given below for more clarification.

Table 01: The research questions

What are the key factors influencing employee engagement and responsibility in the context of cybersecurity in the branch?		
Sub-Question – 1	**Sub-Question – 2**	**Sub-Question – 3**
How do you rate the organization's overall cybersecurity policy which influences your engagement and responsibility in cybersecurity?	How much does the organization's culture encourage employees to be responsible for cybersecurity?	How do you rate the quality of training the organization provides on cybersecurity practices and responsibilities?

Table 01 draws the research questions aimed at understanding the core elements that influence employee engagement and responsibility in cybersecurity within the branch. It provides a clear and focused roadmap for the investigation, allowing for a nuanced exploration of the multifaceted nature of employee engagement and responsibility in cybersecurity within the context of the branch.

1.4 Research Outcome

The outcomes of this research are tailored to be implemented within Pubali Bank Limited, specifically at the Nandina Branch, to enhance cybersecurity through employee engagement. The research findings can also serve as a comprehensive guideline for other banks and financial institutions striving to fortify their digital environments. Thus, the possible outcomes are:

Development of a Cybersecurity Engagement Framework: The research crafts a framework for engaging employees in cybersecurity practices, promoting a culture of responsibility, and encouraging adherence to security protocols.

Identification of Key Factors Influencing Engagement and Responsibility: This study discerns critical elements that affect employee engagement and responsibility toward cybersecurity, offering insights into what motivates or hampers active participation in securing digital environments.

Strategic Recommendations for Enhancing Cybersecurity Practices: Tailored specifically to Pubali Bank Limited, Nandian branch the recommendations cover areas such as policy enforcement, training, and employee incentive structures to foster a security-first mindset.

Potential Roadmap for Industry Application: The outcomes of the research can be generalized to offer a roadmap for other banks and financial organizations to follow. This roadmap can guide institutions in enhancing employee participation in cybersecurity, thereby contributing to the overall robustness of the financial sector's digital landscape.

Contribution to National Cybersecurity Policy and Regulation: Insights from this research are instrumental in shaping national policies and regulations, recognizing the role of human factors in cybersecurity and endorsing practices that cultivate employee engagement and responsibility.

International Implications and Best Practices: The research may yield universally applicable best practices in employee engagement for cybersecurity, providing valuable insights for international banks and regulators.

1.5 The Justification for the Study

The digital age has revolutionized the way banking institutions operate, shifting from traditional face-to-face interactions to digital platforms that offer convenience and efficiency (DeYoung, 2019). At the same time, protecting sensitive financial data, customer information, and transactional systems is vital to ensure trust and maintain stability in the banking sector (International Monetary Fund, 2021). However, the justification for this study is rooted in several interconnected factors which are shown in Figure 02 that underline the urgency and relevance of examining employee engagement and responsibility towards cybersecurity within banking institutions.

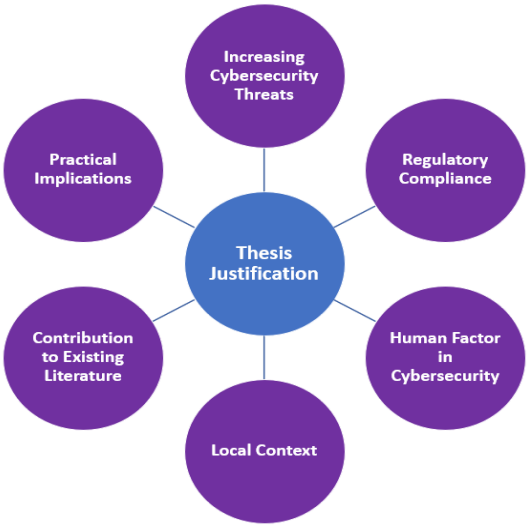

Figure 02: The Study Justification

Increasing Cybersecurity Threats: The complexity and frequency of cyberattacks have surged in recent years, targeting financial data and potentially crippling banking

operations (Symantec, 2020). According to World Economic Forum (2023), the global economic loss due to cybercrime is expected to reach $10.5 trillion by 2025. Understanding employee roles in cybersecurity becomes vital in this context.

Regulatory Compliance: Cybercrime has become a major concern for countries, corporations, and international organizations (World Economic Forum 2023). Governments and international bodies are enforcing stricter regulations to safeguard customer data (Basel Committee on Banking Supervision, 2018). Non-compliance can lead to legal repercussions and reputational damage. Based on the organization's policy, this study can offer insights into aligning employee practices with regulatory or authorization requirements.

Human Factor in Cybersecurity: Studies have shown that human error plays a major role in cybersecurity breaches (KnowBe4, 2020). Therefore, it is crucial to understand how employee engagement and responsibility can reduce these risks (Blythe & Coventry, 2018). By focusing on human behavior, culture and training, organizations can build a more secure digital environment (SDE).

Local Context: Every year, Bangladesh experiences a large number of cyber-attacks, as mentioned above, and investigations show that most of these incidents occur because of human mistakes or errors. Based on this context the topic has been selected for the thesis and it provides an opportunity to explore these concepts within the unique cultural, regulatory, and operational context of the region specifically focusing on Pubali Bank Limited, Nandina Branch.

Contribution to Existing Literature: This research enhances the existing body of knowledge on cybersecurity within the banking industry by introducing a unique perspective that integrates employee engagement with cybersecurity protocols. It emphasizes the importance of the employee's role towards cybersecurity and how human factors can be utilized to bolster security measures in financial institutions. Additionally, it contributes new insights that may foster further research in related fields.

Practical Implications: The urgency to strengthen cybersecurity measures in the banking sector, combined with the vital role of employees in this effort, forms a compelling basis for this study. Findings from this research can guide banking institutions in crafting effective strategies that leverage employee engagement as a tool for enhancing cybersecurity, leading to stronger protection of financial assets and customer data. This study not only adds to academic discourse but also provides practical, actionable insights for professionals in the fields of banking and information security.

1.6 Overview of the Case Company

Pubali Bank Limited was initially launched in 1959 as Eastern Mercantile Bank Limited during East Pakistan period, the bank was established by some Bangalee entrepreneurs under the Bank Companies Act 1913. The goal was to provide credit access to Bangalee entrepreneurs who had limited opportunities for funding from other institutions at the time. After Bangladesh gained independence in 1971, the bank was nationalized according to government policy and renamed Pubali Bank. In 1983, it was again denationalized and became a private entity, taking the name Pubali Bank Limited. From its inception, the bank has played a crucial role in the socio-economic, industrial, and agricultural growth of the country, as well as in overall economic development, by encouraging savings and investing funds (Pubali Bank Limited).

Pubali Bank Limited is one of the most prominent commercial banks in Bangladesh, has a substantial footprint in the banking sector. The digitalization of various services has necessitated a strong focus on cybersecurity measures within the branches of the bank. Pubali Bank Limited, Nandina Branch, is cooperative partner of this research to explore the employee engagement and responsibility toward cybersecurity to ensure an SDE within the bank. As technology advances, the bank must prioritize the establishment of an SDE to safeguard against cyber threats.

Pubali Bank Limited offers a wide array of banking services, including retail and corporate banking, international trade financing, foreign exchange management, and online banking. With its strong commitment to technology-driven services, it provides

digital solutions to cater to the modern banking needs of individuals and businesses (Sarker & Rahman, 2018).

As of 2023, Pubali Bank Limited has a comprehensive network of over 501 branches spread across Bangladesh, with a strategic focus on urban and rural banking. The Nandina Branch, in particular, serves as an essential part of this vast network, catering to the local community (Pubali Bank Limited, 2023).

1.6.1 Corporate Culture and Cybersecurity

The bank's organizational culture emphasizes integrity, accountability, innovation, and customer-centricity. Cybersecurity is an integral part of its operational framework, driven by an alignment between technology and human resources (Ahmed, 2020). The bank maintains a stringent cybersecurity policy and promotes a culture of responsibility and engagement among its employees. The bank's ongoing commitment to digital innovation, coupled with its focus on employee empowerment, renders it an exemplary model for this research.

1.7 Thesis Content

The thesis is organized into six main parts, specifically crafted to explore employee engagement and responsibility toward cybersecurity within Pubali Bank Limited. Below is a detailed breakdown:

Introduction: This chapter provides a comprehensive view of the subject by explaining the background, rationale, an overview of the case company, the objective, research questions, and expected outcomes of the research. It sets the stage for the subsequent exploration of the topic.

Literature Review: The second chapter focuses on reviewing existing literature related to cybersecurity and employee engagement. This chapter helps in defining the main concepts and constructing the theoretical framework tailored to reflect the specificities of the case company.

Research Methodology: This chapter outlines the methodology employed in the research, including the philosophy, approach, methodological choice, research design, data collection plans and methods, and analysis techniques. It serves as the backbone for the research, ensuring rigor and validity.

Descriptive Statistics: The descriptive statistics chapter involves the analysis and interpretation of data to describe its overall features based on the questionnaire. This statistical approach includes measures such as mean, range, standard deviation frequency, and other metrics that help in understanding the key characteristics of a dataset with tables and charts.

Result and Discussion: Chapter five deals with the results and discussion of the study. It delves into the crucial aspects of regression analysis, encompassing model specifications, statistical outcomes, and their interpretation. The aim is to fulfill the research objective by utilizing the collected data.

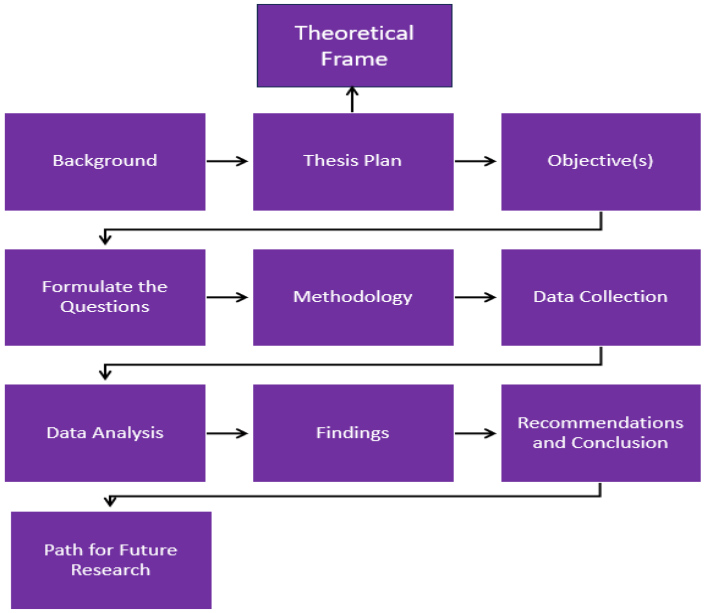

Figure 03: Thesis Structure

Figure 03 shows the structure of this thesis is strategically designed to guide the reader through the nuanced exploration of employee engagement and responsibility in cybersecurity, with a special emphasis on the context of Pubali Bank Limited. It offers a

clear pathway from understanding the theoretical underpinnings to practical applications and insights.

2. LITERATURE REVIEW

Cybersecurity has emerged as a vital area of concern for organizations across various sectors, and it is particularly pronounced in the banking industry due to the sensitivity and value of the financial data handled (Romanosky, 2019). While technological advancements have offered innovative solutions to cyber threats, human aspects, including employee engagement and responsibility, play an essential role in building and maintaining a secure digital environment (SDE) (Beautement, Sasse, & Wonham, 2008).

Research underscores the critical role employees play in ensuring an organization's cybersecurity. The human factor is often deemed as both the weakest link and the first line of defense against cyber threats (Theofanos, Stanton, & Prettyman, 2015). Indeed, Albrechtsen and Hovden's (2010) research indicates that a lack of security awareness among employees is one of the significant challenges in achieving effective cybersecurity. Existing research emphasizes the need to enhance employee engagement and responsibility, but there is a gap in understanding how to effectively foster these aspects within the specific context of banking institutions.

Organizational culture plays a crucial role in promoting employee engagement in cybersecurity. Employees are the main element of the organizational culture which plays a vital role in promoting employee engagement in cybersecurity. Pfleeger and Caputo (2012) argue that the creation of a security-conscious culture is necessary to mitigate cybersecurity risks effectively. A security-conscious culture can encourage positive security behaviors, promote adherence to security policies, and prompt reporting of security incidents (Puhakainen & Siponen, 2010). However, the literature appears to lack an in-depth exploration of how organizational culture and employee engagement intertwine, particularly in the banking sector. This gap underscores the

need for more targeted research to develop strategies that cater to the unique cybersecurity needs of banks.

Training and education are vital components in building security awareness among employees (Rezgui & Marks, 2008). While training programs have been recognized as essential to ensure SDE, there seems to be a gap in understanding the most effective methods for imparting cybersecurity knowledge and engaging employees in the banking context. More research is required to identify the specific needs and strategies for training bank employees, ensuring alignment with organizational goals and industry regulations.

The existing literature highlights the importance of employee engagement and responsibility in cybersecurity, particularly in banking. However, there appears to be a gap in research specifically targeting how to foster these elements within banking institutions. The unique challenges and requirements of banks necessitate a tailored approach to engaging employees in cybersecurity practices. This literature review underscores the need for a comprehensive study focusing on the intersections between employee engagement and responsibility towards cybersecurity, organizational culture, cybersecurity policy, and training within the context of banking to make a secure digital environment (SDE). It paves the way for the current thesis to explore these areas, bridging the identified gaps, and contributing to the existing body of knowledge.

2.1 The Overview of Cybersecurity

Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks, damage, or unauthorized access. It is an essential aspect of technology that is becoming more vital as the amount of data created and stored continues to grow, and the complexity of threats evolves (Cavelty, 2014).

In the banking industry, the significance of cybersecurity is even more pronounced, given the sensitive nature of the information handled. Banks are attractive targets for cybercriminals due to the financial gains involved (Chen et al., 2014). The types of attacks can range from phishing and malware to more complex breaches involving

advanced persistent threats (APTs). This has necessitated a more robust and adaptive approach to cybersecurity in banking (Mansfield-Devine, 2016).

Governments and regulatory bodies have responded to these growing threats by implementing strict regulations and standards that banks must adhere to, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Federal Information Security Modernization Act (FISMA) in the United States (Kaplan et al., 2016). These standards require banks to implement rigorous security measures and regular audits to ensure compliance.

Figure 04: The NIST Cybersecurity Framework (NIST, 2018)

The National Institute of Standards and Technology (NIST) of United States has given a role by the Cybersecurity Enhancement Act of 2014 (CEA) to create guidelines for managing cybersecurity risks. The institution has given proper guidelines, known as the ***Cybersecurity Framework*** that shown in Figure 04, allow businesses including financial institutions to protect themselves without needing new regulations and using a flexible, cost-effective approach. The Cybersecurity Framework also aligns with globally recognized standards, promoting international cooperation on Cybersecurity (NIST 2018). In the report, the NIST has emphasized the importance of Cybersecurity for every organization those are providing e-services

However, there has been a shift in recognizing cybersecurity not just as a technological issue but a business one, impacting reputation, customer trust, and overall business sustainability (Gordon et al., 2015). The focus is also on the human aspect of cybersecurity, with employee training and awareness being vital components in preventing breaches (Parsons et al., 2017). With technology and cyber threats

continuing to evolve, cybersecurity must be an ongoing effort, continuously adapting to new risks and challenges. As Böhme (2010) asserts, the nature of cybersecurity is dynamic, and the protection measures must reflect this dynamic nature to be effective.

2.2 Employee Engagement and Responsibility

Employee engagement and responsibility are vital components in the cybersecurity landscape, particularly in industries that handle sensitive information, such as banking. Engagement and responsibility are not just theoretical constructs; they are measurable and can be enhanced through targeted interventions. Many organizations use metrics and benchmarks to gauge employee engagement and responsibility in cybersecurity (Von Solms & Van Niekerk, 2013). Several factors influence the level of employee engagement and responsibility towards cybersecurity which has been shown in Figure 05.

Figure 05: Factors that Influence Cybersecurity

Organizational culture, leadership, training, and awareness of cybersecurity policies and practices play significant roles (Albrechtsen & Hovden, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010). Modern research and practice demonstrate that understanding these factors can empower organizations to bolster their cybersecurity defenses.

2.3 Organizational Policy and Cybersecurity

Organizational policies play a vital role in defining, shaping, and enforcing cybersecurity within a company. They lay the groundwork for protecting an organization's assets, data, and reputation by prescribing the rules, standards, and guidelines that must be followed by all employees and stakeholders. Policies are vital as they serve to define

the acceptable and unacceptable use of resources, establishing clear guidelines for behavior and actions in the digital sphere (SANS Institute, 2014). Organizational policies serve as a compass that guides employee behavior and decision-making related to information security (Siponen et al., 2014). They formalize the expectations of management regarding acceptable practices, align with regulatory compliance, and support the strategic objectives of the organization (Herath & Rao, 2009). Effective cybersecurity policies often include:

- Purpose and Scope
- Responsibilities
- Standards and Procedures
- Incident Response Plan
- Compliance and Enforcement

The Implementing cybersecurity policy is not without challenges. Common obstacles such as:

- **Lack of Awareness**: The lack of awareness among employees about the policy or its significance (Bulgurcu et al., 2010) can lead individuals astray, creating opportunities for cybercriminals.
- **Resistance to Change**: Staff resistance to new rules and procedures (D'Arcy et al., 2009) can create challenges in implementing cybersecurity measures.
- **Alignment with Organizational Culture**: Aligning the policy with the organizational culture and values is essential for effective cybersecurity measures (Whitman & Mattord, 2018).

2.4 Organizational Culture and Cybersecurity

Organizational culture, defined as the shared values, beliefs, and practices that shape the behavior of individuals within an organization, is an integral part of cybersecurity. It influences how employees perceive, interact with, and adhere to cybersecurity policies and procedures. Organizational culture plays a significant role in shaping employees' attitudes and behaviors towards cybersecurity (Da Veiga & Eloff, 2010). A positive

organizational culture that emphasizes cybersecurity can foster a proactive approach to threat detection and mitigation. Employees in such a culture are more likely to comply with security protocols, report suspicious activities, and contribute to continuous improvement in cybersecurity practices (Dang-Pham & Pittayachawan, 2015). Conversely, a culture that disregards or minimizes the importance of cybersecurity may lead to negligence, non-compliance, and increased vulnerability to cyber threats (Kraemer & Carayon, 2007). A culture that prioritizes security can foster a more robust defense against cyber threats.

2.5 Organizational Training in Cybersecurity

Organizational training in cybersecurity is a crucial aspect of a company's overall security posture. As cyber threats continue to evolve, so too must the skills and awareness of the employees responsible for safeguarding an organization's assets. With human error being one of the primary causes of security breaches (Kaspersky, 2019), training is essential for reducing the likelihood of successful cyber-attacks. It helps to build a culture of security awareness, encourages adherence to organizational policies, and equips employees with practical skills to respond to incidents (Parsons et al., 2017). Effective training and support in cybersecurity can equip employees with the knowledge, skills, and confidence required to recognize and mitigate potential threats. Training is a continuous process, especially for cybersecurity that arranged by the organizations based on their needs which shown in Figure 06.

Figure 06: Training Process

Figure 06 indicates that an organization should conduct cybersecurity training sessions for its employees and continuously monitor their performance. The organization then assesses the performance standards using various tools and techniques. Based on the evaluation, selected employees might undergo additional short or long-term training for further development.

2.6 Theoretical Framework for the Case Company

The theoretical framework for this thesis integrates contemporary or modern theories and concepts related to understanding the dynamics of employee engagement and responsibility, organizational culture, cybersecurity policy, and training within the banking environment. This synergy of theories forms the bedrock for the thesis work in cooperation with the case company.

2.6.1 Employee Engagement and Responsibility Theory

The framework for employee engagement and responsibility is founded on the Self-Determination Theory (SDT) by Deci and Ryan (2000), which emphasizes autonomy, competence, and relatedness as key factors in driving engagement and personal responsibility towards cybersecurity (Gagné & Deci, 2021). Engagement is also explored through the lens of Kahn's (1990) Engagement Theory, highlighting how employees bring themselves physically, cognitively, and emotionally to their work roles. A sense of responsibility towards cybersecurity may further be informed by the Theory of Planned Behavior (Ajzen, 1991), emphasizing attitudes, subjective norms, and perceived behavioral control. The studies recognize the importance of employees' active engagement and responsibility in ensuring a secure digital environment (SDE).

2.6.2 Cybersecurity Policy Theory

The framework integrates the modern theory based on the topic. Cybersecurity policy is explored using the Policy Compliance Model, which examines how awareness, attitude, and norms influence policy adherence (Ifinedo, 2022). The model recognizes that policy compliance is multifaceted and can be influenced by individual and organizational factors (Puhakainen & Siponen, 2021). Additionally, the influence of the organization's

cybersecurity policy is explored, considering frameworks such as the NIST Cybersecurity Framework (NIST, 2018) that shown in Figure 04. These theories also denoted the classical theory, Protection Motivation Theory (Rogers, 1975) to understand the psychological factors driving employees to adhere to cybersecurity policies. A study by Mishra and et al., (2022) identifies ten (10) prevalent cybersecurity aspects, as depicted in Figure 07, from various pertinent literatures.

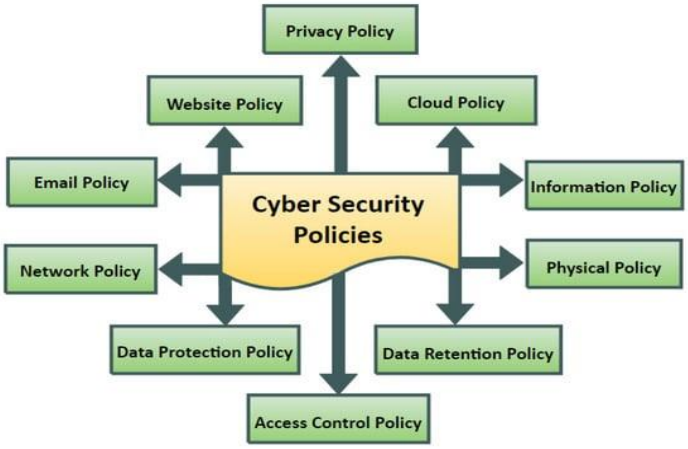

Figure 07: Cybersecurity Policies Taxonomy (Mishra and et al., 2022)

A robust cybersecurity policy can enhance the secure digital environment (SDE) by leveraging psychological principles to foster a sense of responsibility and compliance among employees.

2.6.3 Organizational Culture Theory

Organizational culture is examined through Schein's (2010) Organizational Culture Model, considering underlying assumptions, shared values, and common practices within an organization. This model helps explore how the organizational culture of the bank promotes or hampers the focus on cybersecurity. Recent work on organizational culture emphasizes the importance of an adaptive and proactive cybersecurity culture (Herath & Rao, 2022).

In a recent study by MIT $(IC)^3$ in 2017, establishing a cybersecurity culture is emphasized as vital for organizations. Current $(IC)^3$ research underscores the factors that mold this culture that shows in Figure 08. Managers must recognize these

'managerial levers' for resource allocation. Moreover, $(IC)^3$ researchers present a strategy that transitions from relying solely on tech specialists to ensuring everyone takes personal responsibility for cybersecurity.

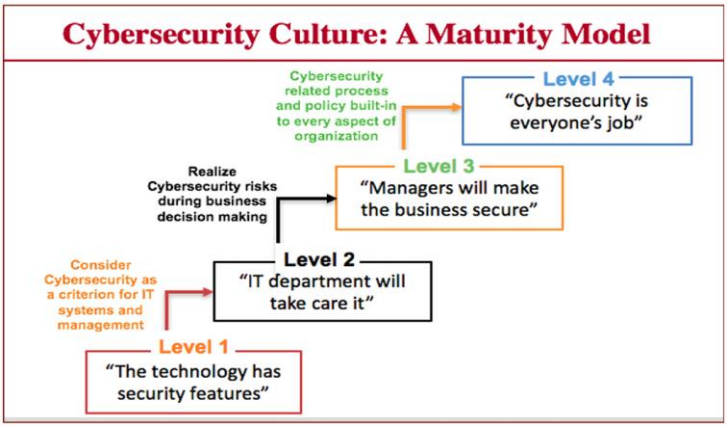

Figure 08: A roadmap to increase resilience by creating a mature culture of cybersecurity (MIT (IC)3 (2017)

This framework incorporates a culture-centric approach that recognizes how organizational norms and values shape cybersecurity behavior (Gallagher & Gallagher, 2020). These studies reveal that a strongly committed culture can ensure a better SDE in an organization.

2.6.4 Training and Development Theory

The theoretical framework for training in cybersecurity incorporates both classical and modern perspectives. The foundational understanding from Adult Learning Theory (Knowles, 1984) highlights the unique learning needs and preferences of adults, which is further nuanced by contemporary insights into adult learning in technology-driven environments (Gagné & Deci, 2021). Alongside this, the Technology Acceptance Model (TAM), originating from Davis (1989) and later extended by Venkatesh & Davis (2000), emphasizes the critical role of perceived usefulness and ease of use in technology adoption. This perspective is melded with Kirkpatrick's four levels of training evaluation (Kirkpatrick, 1994), which has been integrated with modern evaluations of cybersecurity training effectiveness (Gallagher & Gallagher, 2020). The theoretical framework integrates these diverse elements to provide a comprehensive view of how cybersecurity training can be designed, implemented, and evaluated to meet the

dynamic needs of today's workforce. This synthesis reflects an ongoing evolution in understanding, aligning traditional concepts with contemporary insights to explore how training in cybersecurity can enhance employee engagement and responsibility towords cybersecurity to ensure SDE and organizational resilience in an increasingly interconnected and rapidly changing digital landscape.

2.6.5 Regression Model Theory

Regression analysis, a fundamental statistical method, is used to model the relationship between a dependent variable and one or more independent variables by fitting a linear equation to observed data (Neter, Wasserman, & Kutner, 1990). The basic regression theory involves the analysis of the relationship between a dependent variable and one or more independent variables (Montgomery, Peck, & Vining, 2012). A multiple linear regression model extends the basic linear regression model to include more than one independent variable. The model can be represented by the following equation:

$$y=\beta 0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+ \epsilon$$

Where:

- y is the dependent variable.
- x_1,x_2, and x_3 are the independent variables.
- β0 is the intercept.
- β_1,β_2, and β_3 are the coefficients for the independent variables.
- ϵ is the random error term.

The goal of multiple linear regression is to model the relationship between several independent variables and a dependent variable. By fitting this model to data, it is possible to determine how each independent variable contributes to the variability in the dependent variable, considering the effects of the other independent variables (Kutner, Nachtsheim, Neter, & Li, 2004). In the context of this research on cybersecurity, a multiple linear regression model serves as a statistical framework to analyze how factors such as organizational culture, cybersecurity policy, and training might influence

the employee engagement and responsibility towards cybersecurity within the organization to ensure secure digital environment (SDE).

These theoretical frameworks encapsulate current academic thinking on the intertwined aspects of employee engagement and responsibility, organizational culture, policy, and training within the realm of cybersecurity. It provides a robust foundation for the case study, bridging existing theory with new insights to contribute to the broader field of cybersecurity research.

3 RESEARCH METHODOLOGIES

After evaluating various pieces of methodological literature, this thesis opted to utilize the General Research Process Model for the selected topic. This systematic approach provides a structured exploration into the relationship between employee engagement and responsibility in cybersecurity and organizational policy, culture and training within the selected bank. This structured method includes identifying the problem, reviewing literature, selecting methodology, collecting and analyzing data, and drawing conclusions those show in Figure 09.

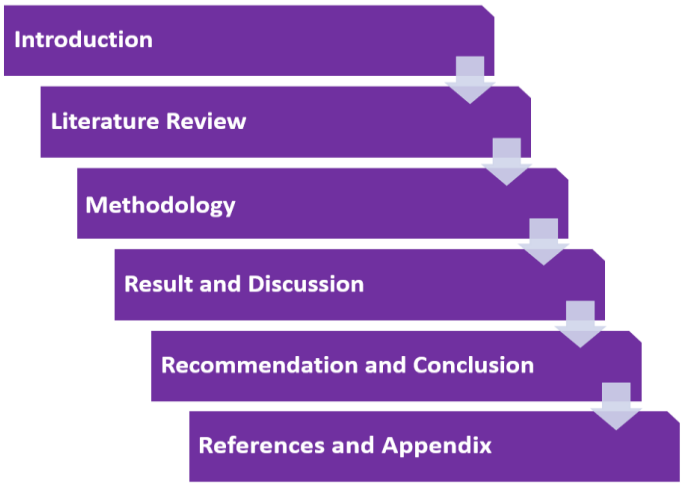

Figure 09: General Research Process Model

By following this approach, the research is conducted methodically, offering nuanced insights into the relationship between employee engagement, responsibility, and cybersecurity within banking. The process allows for rigorous analysis, adaptability to

various methods, ethical considerations, and clear communication of findings. The structured nature of the model ensures relevance to both industry and academia, contributing to understanding and practical applications in the banking industry, making it an apt approach for such a complex and specific subject.

3.1 Research Philosophy

This study follows the positivist paradigm, using quantitative methods to systematically investigate the relationships between organizational cybersecurity policy, culture, training, and engagement and responsibility of the employee towards cybersecurity within selected branch (Creswell & Creswell, 2018). The positivist paradigm is based on the belief that reality is fixed and can be measured objectively. It often aligns with the scientific method, focusing on hypothesis testing, measurement, objectivity, and causality. In this paradigm, the researcher often plays a detached and neutral role, seeking to uncover universal laws or truths.

3.2 Research Approach

The study employs a quantitative research approach, utilizing survey methods to collect data on the predetermined variables related to employee engagement and responsibility in cybersecurity. This approach allows for statistical analysis and generalization of findings (Bryman, 2016). The quantitative method being employed in this study facilitates the collection of empirical data, subject to statistical analysis. Multiple linear regression is being used as the analytical technique, enabling the investigation of the simultaneous effects of multiple independent variables on a dependent variable.

A survey questionnaire is given to all the employees at the selected bank branch. This questionnaire is designed to capture key metrics related to employee engagement and responsibility in maintaining a Secure Digital Environment (SDE) for cybersecurity. The survey is made in a clear and uniform way, so the answers from different people can be easily compared.

The quantitative approach, the survey method, and the use of multiple linear regression align seamlessly with the research objectives and provide a robust framework for

examining the collected data within the chosen context. The insight derived from this approach contributes valuable empirical evidence to the field, potentially informing future strategies and policies within the banking industry.

3.3 Methodological Choice

A quantitative research design has been chosen, with survey questionnaires employed to collect data to populate the regression model. The survey questionnaire is structured and designed carefully to make sure that the information collected from different people can be easily compared. The use of this standardized method aims to make the data collection process both consistent and reliable. Researchers have found that this approach helps to ensure that the results of the study can be trusted (Saunders et al., 2009). By following a well-planned method, the thesis aims to provide valuable insights into the subject being studied.

3.4 Research Model

The research model serves as a vital framework for understanding the connections between the variables involved in the study. The relationship between the dependent and independent variables is carefully expressed and analyzed using multiple linear regression. This statistical method allows for examining various factors that could influence the outcome, providing a comprehensive view of the subject. The regression equation has been employed to structure the research model for this thesis, forming a systematic and logical basis for the investigation.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \epsilon$$

Where:

Y: Employee Engagement and Responsibility in Cybersecurity

X_1: Organizational Cybersecurity Policy

X_2: Organizational Culture on Cybersecurity

X_3: Training on Cybersecurity

Based on the regression equation the research model of the thesis has been structured below.

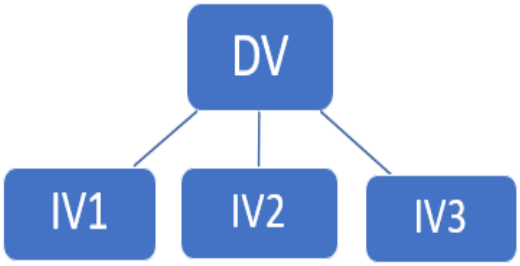

Figure 10: Research Model

Figure 10 shows that the relationship between dependent variable (DV) and independent variable (IV). In this thesis the dependent variable is employee engagement and responsibility in cyberbersecuriy and the independent variables are the organizational policy, the organizational culture, and the organizational training which can lead a secured digital environment for the selected branch and other organizations as well.

In light of the research model, this study aims to validate the alternative hypothesis (H_1), which is formally stated as follows:

Alternative Hypothesis (H_1): At least one of the independent variables significantly influences employee engagement and responsibility in cybersecurity.

3.5 Research Design

Research Design serves as the blueprint for the entire research process. It outlines the procedures for collecting, analyzing, and interpreting data, and guides the researcher in understanding and exploring the specific research problem. A well-constructed research design ensures that the gathered information accurately addresses the research question, making the study both valid and reliable. In this section, the chosen research design for the thesis is elaborated, highlighting its appropriateness and methodological considerations.

The research unfolds within the organizational context of Pubali Bank Limited, Nandina Branch, providing a real-world perspective on cybersecurity within the banking sector. Administered electronically, the survey captures insights from a representative sample of employees across various departments and hierarchical levels, ensuring a holistic view of the bank's cybersecurity policy, culture, and training. These subjects, being active employees, offer a range of insights: from their engagement and responsibility levels regarding cybersecurity practices to their inherent attitudes toward these practices, encapsulating feelings, beliefs, and behavioral intentions. Such an encompassing study design promises to address the diverse intricacies of the role of employee engagement and responsibility towards cybersecurity to ensuring a secure digital environment (SDE) (Smith & Jones, 2021).

The dependent variable is employee engagement and responsibility in the context of cybersecurity, while the independent variables include organizational cybersecurity policy, organizational culture, and training. The variables list is given below:

Table 02: List of Variables

Dependent Variable	Independent Variables
Employee Engagement and Responsibility in Cybersecurity	Organizational Cybersecurity Policy
	Organizational Culture on Cybersecurity
	Training on Cybersecurity

Table 02 presents the key variables of the study. The dependent variable is "employee engagement and responsibility in cybersecurity." This variable analyzes in relation to three independent variables: the rating of organizational cybersecurity policy, the extent of organizational culture promoting responsibility, and the rating of training quality. These independent variables are crucial factors that examines based on the data collected to understand their potential influence on employee engagement and responsibility in the context of cybersecurity.

The action plan for this thesis starts with a review of the existing literature on the topic which creates gaps and opportunities for further research. It helps to build a theoretical framework and identify key areas for the study. Next, studying related data and information to get insights regarding cybersecurity, a questionnaire is designed to gather

specific information from employees in the selected bank branch. The collected data is then analyzed using multiple linear regression to understand how employee engagement affects cybersecurity. Later on, this analysis leads to the identification of key insights and the preparation of a final report, detailing the findings and offering strategic recommendations. Ultimately, the research provides insights into enhancing cybersecurity within the selected branch to ensure a secure digital environment (SDE). These findings and recommendations may also benefit other organizations in similar contexts.

A survey questionnaire is developed to gauge employees' levels of engagement, responsibility, and attitudes toward cybersecurity practices. The questionnaire consists of validated scales and items adapted from current literature. It is administered electronically to a representative sample of employees across various departments and hierarchical levels within the Pubali Bank Limited, Nandina Branch. The survey ensures the confidentiality and anonymity of respondents, promoting truthful and precise feedback.

The primary source of data for this research is the employees of Pubali Bank Limited, Nandina Branch. Given the focus on employee engagement and responsibility towards creating a Secure Digital Environment (SDE), firsthand information from these staff members is vital. The type of data is quantitative, collected through structured questionnaires. This quantitative data enables the application of statistical methods, specifically multiple linear regressions, to ascertain the relationship between employee engagement and their responsibility in ensuring cybersecurity.

The population for this research comprises all employees working at the Pubali Bank Limited, Nandina Branch. Since the aim is to get an in-depth understanding of the entire branch's perspective on the topic at hand, the sample for this study includes all employees of the said branch. Including all employees ensures that the results are representative of the entire population, eliminating the need for random sampling.

Structured questionnaires serve as the primary data collection tool. These questionnaires are designed with a combination of Likert scale questions, multiple-choice questions, yes-no and open-ended questions to capture varying levels of employee engagement and responsibility towards cybersecurity in the bank. To ensure validity and reliability, the questionnaire is pre-tested before distribution to the selected branch.

Data collection commenced on and is set to conclude by 07th October 2023, spanning a total of six weeks. The first week involves distributing the questionnaires to the employees, with reminders sent in the subsequent weeks. By the end of the designated period, all completed questionnaires are returned. During this period, periodic checks are conducted to monitor response rates, ensuring maximum employee participation.

Figure 11: Research Design

Figure 11 illustrates the interconnected components integral to the research design. It encompasses critical factors such as setting and subjects features, variable identification, questionnaire design, planning the framework, sampling strategy, and primary data collection. These strategic steps collectively contribute to the acquisition of data, facilitating subsequent analysis to fulfill the objectives of the study.

3.6 Data Analysis

Upon collecting all the data, it is entered into a suitable statistical software package, such as MS Excel and JASP 0.18.0.0, for analysis. The primary analytical method is multiple linear regressions, which helps in understanding how different factors related to employee engagement predict their responsibility towards cybersecurity in the bank. Descriptive statistics provide an overview of the data, including measures of central tendency and dispersion. Assumptions for the regression analysis are checked, followed by building, testing, and interpreting the regression model. This analysis covers the objectives and questions of the thesis and also aims to inform the bank's policies, culture and training programs on cybersecurity, ensuring that they effectively engage their employees in maintaining a secure digital environment.

3.7 Interpretation of Data

The collected numerical data is analyzed through the utilization of a linear regression model. In this approach, the linear regression model allows for the examination of relationships between variables, with an emphasis on identifying patterns, correlations, and trends within the dataset. This method helps in understanding the extent to which independent variables influence a dependent variable.

3.8 Ethical Considerations

Ethical considerations are of utmost importance throughout the research process. The study adheres to ethical guidelines and seeks institutional research ethics approval if required. The following ethical considerations are addressed:

Participants are provided with detailed information about the study's purpose, procedures, and potential risks and benefits. Their voluntary participation and right to withdraw at any stage are emphasized and informed consent is obtained from all participants.

Participants' confidentiality and anonymity are strictly maintained. Data is stored securely and only accessible to the research team. Participants' identities are protected by assigning pseudonyms to ensure anonymity..

Data collected during the study is handled in compliance with relevant data protection regulations. Measures are implemented to safeguard the security and privacy of participants' information.

Participants' privacy is respected throughout the research process. They are assured that their responses and personal information are treated with confidentiality and used solely for research purposes.

4. DESCRIPTIVE STATISTICS

This study is conducted with the aim of evaluating employee engagement and responsibility in the context of Cybersecurity. It examines the influence of organizational policy, organizational culture, and training on these aspects. Data for this analysis was collected via a survey questionnaire from the Nandina Branch of Pubali Bank Limited in Bangladesh.

4.1 Demographical Details of the Respondents

The study involved a total of 18 respondents, and their demographic information was collected as part of the survey questionnaire. This demographic section encompassed details about their gender, age, job position, and job experience. It's worth noting that within the selected branch, there were two additional employees who were not involved in roles related to organizational cybersecurity and were thus excluded from this particular study. Importantly, the data collection process for the demographic details of the respondents was thorough and complete, with no missing data, ensuring the reliability and comprehensiveness of the dataset.

Table 03: Gender of the Employees

Gender	Frequency	Percent	Valid Percent	Cumulative Percent
Male	11	61.111	61.111	61.111
Female	7	38.889	38.889	100.000
Missing	0	0.000		
Total	18	100.000		

Table 03 displays the gender distribution among the 18 individuals in the study. It features two categories: Male and Female, with 11 males and 7 females in the sample. The percentages are calculated based on the total sample size, where males constitute 61.111%, and females account for 38.889% of the sample. Notably, there are no missing data points in the gender variable.

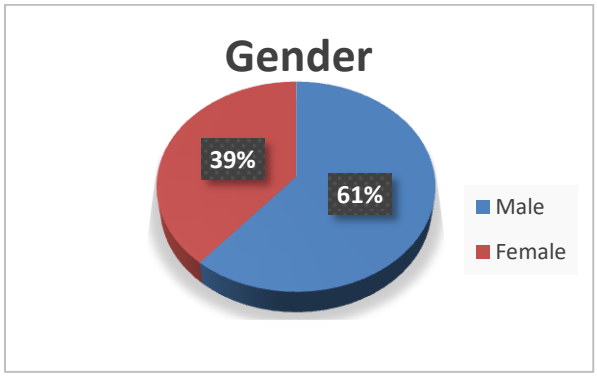

Figure 12: Gender of the Employees

Based on the data from Table 03, Figure 12 shows a pie chart that represents the gender distribution within the study, involving a total of 18 individuals. The chart illustrates that 61% of the study participants are male, while the remaining 39% are female which provides a clear visual insight into the gender composition of the sample.

Table 04: The Age Range of the Employees

Age	Frequency	Percent	Valid Percent	Cumulative Percent
20-29	2	11.111	11.111	11.111
30-39	10	55.556	55.556	66.667
40-49	4	22.222	22.222	88.889
50-59	2	11.111	11.111	100.000
Missing	0	0.000		
Total	18	100.000		

Table 04 categorizes respondents into four age groups: 20-29, 30-39, 40-49, and 50-59. It indicates the number of respondents within each category, with two in the 20-29 age range, ten in the 30-39 category, four in the 40-49 group, and two in the 50-59 range. Where, 11.111% fell into the 20-29 category, 55.556% in the 30-39 group, 22.222% in the 40-49 segment, and 11.111% in the 50-59 range.

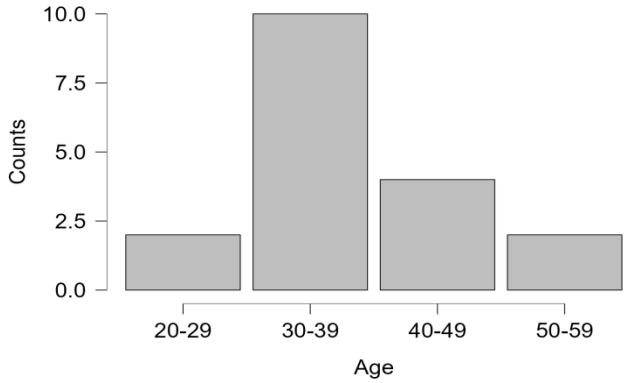

Figure 13: Age Range of the Employees

Based on the data in Table 04, Figure 13 visually presents a column chart depicting the age distribution of employees. The chart clearly illustrates that the most prominent age category among employees is 30-39, while the age ranges of 20-29 and 50-59 are the least represented. Additionally, the age category of 40-49 is less than 30-39 and more than 20-29 and 50-59 which easily overview of the employee age distribution within the study.

Table 05: Job Position of the Employees

Job Position	Frequency	Percent	Valid Percent	Cumulative Percent
Junior Officer	5	27.778	27.778	27.778
Officer	3	16.667	16.667	44.444
Senior Officer	3	16.667	16.667	61.111
Principal Officer	5	27.778	27.778	88.889
Manager	1	5.556	5.556	94.444
Other	1	5.556	5.556	100.000
Missing	0	0.000		
Total	18	100.000		

Table 05 provides a comprehensive overview of the job positions held by employees, encompassing various categories including Junior Officer, Officer, Senior Officer, Principal Officer, Manager, and Other (Deputy Junior Officer). The table reveals the distribution of respondents across these job positions, with five respondents occupying roles as Junior Officers and five as Principal Officers, three respondents working as Officers and three as Senior Officers, in addition to one respondent serving as a Deputy Junior Officer and another in the capacity of a Branch Manager. The "Percent" column quantifies the proportion of respondents within each job position relative to the total sample size of 18.

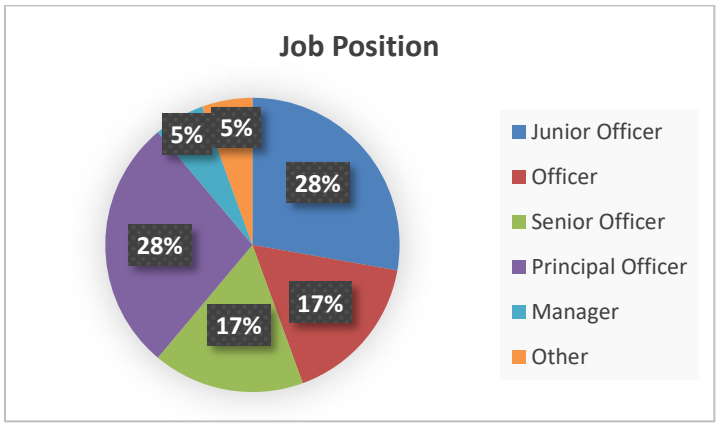

Figure 14: Job Position of the Employees

Building upon the data from Table 5, Figure 14 visually represents the job positions held by employees within the branch through a pie chart. The chart vividly illustrates that Junior Officers and Principal Officers collectively constitute the most significant portion, each accounting for 28% of the total workforce. Additionally, 17% of employees serve as both Officers and Senior Officers, while 5% occupy other roles within the branch. This pie chart offers a clear and intuitive visualization of the distribution of job positions among employees, facilitating a comprehensive understanding of the branch's employment landscape.

Table 06: Job Experience of the Employees

Experience	Frequency	Percent	Valid Percent	Cumulative Percent
1-5	6	33.333	33.333	33.333
6-10	3	16.667	16.667	50.000
11-15	7	38.889	38.889	88.889
21-25	1	5.556	5.556	94.444
26-30	1	5.556	5.556	100.000
Missing	0	0.000		
Total	18	100.000		

Table 06 provides an insight into the job experience of the study's respondents, classifying them into five distinct experience ranges: 1-5 years, 6-10 years, 11-15 years, 21-25 years, and 26-30 years. Specifically, 6 respondents possessed 1-5 years of experience, 3 respondents had 6-10 years, 7 respondents held 11-15 years of experience, while 1 respondent had 21-25 years of experience, and 1 respondent boasted 26-30 years of experience.

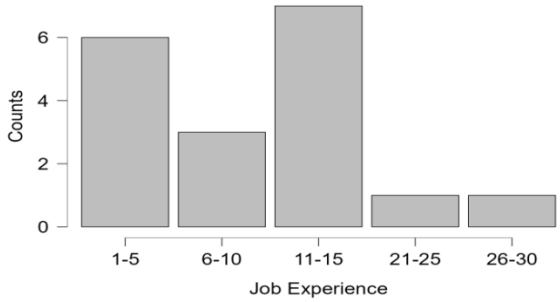

Figure 15: Job Experience of the Employees

Derived from the data presented in Table 6, Figure 15 visually communicates the distribution of job experience among the study's respondents through a column chart. The chart distinctly highlights that the most prevalent job experience category is 11-15 years, while 21-25 years and 26-30 years represent the least common experience ranges in the chart. Notably, the chart indicates a substantial percentage of employees possessing 6-10 years of experience.

4.2 Engagement and Responsibility towards Cybersecurity

The table below presents descriptive statistics related to engagement and responsibility in the context of cybersecurity. It offers valuable insights into the participants' practice and understanding in this domain.

Table 07: Descriptive Statistics of Engagement and Responsibility to Cybersecurity

	Practice	**Understanding**
Valid	18	18
Missing	0	0
Mean	4.611	4.333
Std. Deviation	0.608	0.594
Minimum	3.000	3.000
Maximum	5.000	5.000

Table 07 represents a statistical overview of engagement and responsibility towards cybersecurity, focusing on two dimensions: "Practice" and "Understanding." Among the 18 participants, there are no missing data points, ensuring a complete dataset. The Mean values indicate the average scores, with practice having a mean of 4.611 and understanding slightly lower at 4.333, providing insight into the central tendency of engagement and responsibility in the realm of cybersecurity. Additionally, the Std.

Deviation measures the variability, with practice exhibiting a moderate degree at 0.608, while understanding shows a slightly lower variability at 0.594. The Minimum and Maximum values establish the score range, which spans from 3.000 to 5.000 for both practice and understanding. This table furnishes essential statistics to comprehend the participants' engagement and responsibility levels in the cybersecurity context, encompassing central tendencies, variability, and the score range.

Table 08: Practice of Cybersecurity in the Organization

CS Practice	Frequency	Percent	Valid Percent	Cumulative Percent
4	5	27.778	27.778	27.778
5	12	66.667	66.667	94.444
3	1	5.556	5.556	100.000
Missing	0	0.000		
Total	18	100.000		

Table 8 provides a comprehensive overview of cybersecurity practices within the organization to ensure a secure digital environment (SDE), presented as a frequency distribution. The scale ranges from the lowest value, 1, to the highest value, 5, on a Likert scale. In this dataset, the selected ratings span from 3 to 5, encompassing a total of 18 responses. Among these responses, only 1 individual, constituting 5.556% of the total, rated the organization's cybersecurity practices as 3. A more common rating of 4 was assigned by 5 respondents, accounting for 27.778% of the total responses. Notably, the majority of participants, precisely 12, conferred a rating of 5, representing 66.667% of the total responses. It's noteworthy that there were no missing or incomplete responses in this dataset, ensuring a comprehensive and complete representation of cybersecurity practices within the organization.

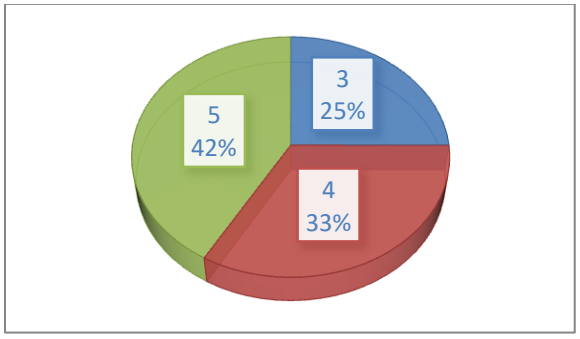

Figure 16: Cybersecurity Practice in the Organization

Building upon the data from Table 8, Figure 16 visually illustrates how respondents have rated their organization's cybersecurity practices using a pie chart. The chart clearly shows that most respondents have given high ratings, specifically 5 and 4, with a significant number opting for the top rating. This could indicate a high level of confidence in the cybersecurity practices within these organizations which plays a crucial role in ensuring a secure digital environment (SDE) of the organization. Importantly, it's worth mentioning that only a minority of employees have chosen to rate their organization's cybersecurity practices as 3, signifying that a smaller portion of respondents are less certain about this aspect.

Table 09: Understanding the Levels of Cybersecurity Breach

Understanding	Frequency	Percent	Valid Percent	Cumulative Percent
Neutral	1	5.556	5.556	5.556
Agree	10	55.556	55.556	61.111
Strongly Agree	7	38.889	38.889	100.000
Missing	0	0.000		
Total	18	100.000		

Table 09 displays responses to a survey question about understanding cybersecurity breach levels. Respondents had five options: "Strongly Disagree," "Disagree," "Neutral," "Agree," and "Strongly Agree." Only one respondent (5.556%) selected "Neutral." The majority, 10 or (55.556%) chose "Agree," and a significant number, 7 or (38.889%) opted for "Strongly Agree." No responses were missing. This indicates a high level of understanding among the respondents regarding cybersecurity breach levels.

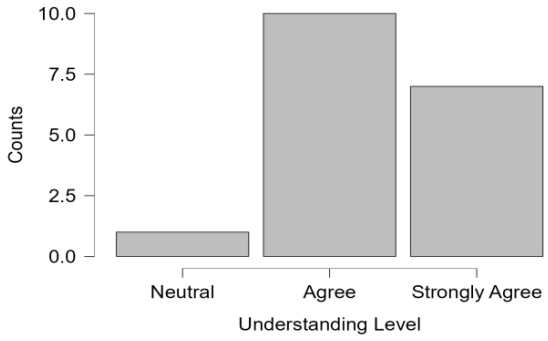

Figure 17: Understanding Levels of Cybersecurity Breach by the Employees

Figure 17, derived from the data in Table 9, presents a column chart depicting employees' understanding of cybersecurity breach levels within the organization. Here it’s clear that the majority are “Strongly Agree” and “Agree” that they have high level of understanding regarding cybersecurity breach which is more important to secure the digital environment of the branch. Only a few respondents are "Neutral" on this matter.

4.3 Cybersecurity Policy for Engagement and Responsibility

The table below offers descriptive statistics for the organization's cybersecurity policy and its impact on employee engagement and responsibility in the cybersecurity context, providing valuable insights into the policy's effectiveness.

Table 10: Descriptive Statistics of Cybersecurity Policy of the Organization

	Familiar with the Policy	Influenced by the Policy
Valid	18	18
Missing	0	0
Mean	4.333	4.556
Std. Deviation	0.485	0.616
Minimum	4.000	3.000
Maximum	5.000	5.000

Table 10 provides statistical information on two dimensions: a) familiarity with the organization's cybersecurity policy, and b) the policy's influence on employee engagement and responsibility in the cybersecurity context. Regarding familiarity with the policy, the respondents provided an average rating or mean of 4.333, with a standard deviation of 0.485, indicating limited variation in responses. Ratings for this dimension ranged from a minimum of 4 to a maximum of 5. In contrast, when considering the policy's influence on employee engagement and responsibility, the average rating was slightly higher at 4.556, with a higher standard deviation of 0.616, signifying greater response variability. Ratings for this aspect ranged from a minimum of 3 to a maximum of 5. These findings suggest that except a few, most of the respondents generally understand and are influenced by the organization's cybersecurity policy.

Table 11: Familiar with the Cybersecurity Policy of the Organization

Familiar with the CS Policy	Frequency	Percent	Valid Percent	Cumulative Percent
Familiar	12	66.667	66.667	66.667
Very Familiar	6	33.333	33.333	100.000
Missing	0	0.000		
Total	18	100.000		

Table 11 provides an overview of respondents' familiarity with the organization's cybersecurity policy. Respondents had the option to choose from five levels of familiarity: "Very Unfamiliar," "Unfamiliar," "Neutral," "Familiar," and "Very Familiar." Here, 12 respondents selected "Familiar," signifying their familiarity with the cybersecurity policy. Additionally, 6 respondents opted for "Very Familiar," indicating a high level of familiarity with the organizational policy in the context of cybersecurity. It's worth noting that there were no missing responses in this survey.

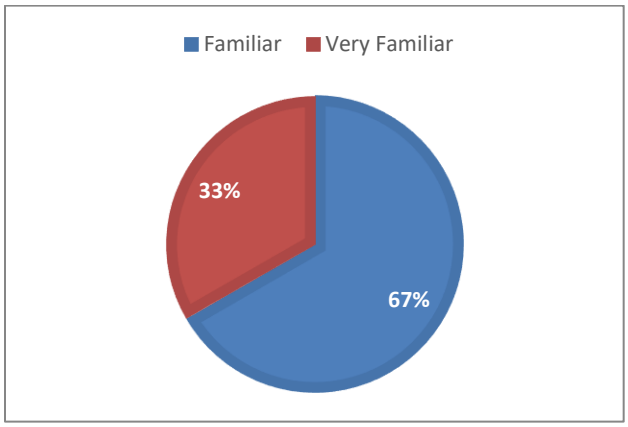

Figure 18: Familiar with the Cybersecurity Policy of the Organization

Utilizing the data from Table 11, Figure 18 visually represents employees' familiarity with the organization's cybersecurity policy through a pie chart. The chart indicates that 67% of employees are "Very Familiar" with the organization's cybersecurity policy, while 33% are "Familiar" with it. This chart strongly suggests that all respondents or employees possess some level of familiarity with their organization's cybersecurity policy, and a significant majority is very familiar with it which is badly needed to maintain a secure digital environment (SDE) of the branch.

Table 12: Cybersecurity Policy for Employee Engagement and Responsibility

Cybersecurity Policy	Frequency	Percent	Valid Percent	Cumulative Percent
4	6	33.333	33.333	33.333
5	11	61.111	61.111	94.444
3	1	5.556	5.556	100.000
Missing	0	0.000		
Total	18	100.000		

Table 12 provides a frequency distribution detailing responses to a survey question concerning the cybersecurity policy of the selected branch, particularly how its role makes the employees engaging and responsible for ensuring a secure digital environment (SDE). The Likert scale employed for responses spans from the lowest value, 1, to the highest value, 5. The data contains valid responses from 18 participants, with no missing data. In the responses, one participant (5.556% of the total) rates the policy as 3, where a majority of participants (61.111%) assigns the highest rating of 5, and an additional 33.333% provides a rating of 4. This distribution reflects the effectiveness of the cybersecurity policy in fostering the employees' engagement and responsibility within the organization for a secure digital environment.

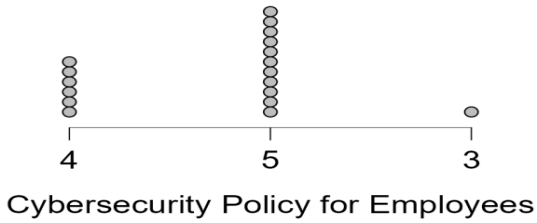

Figure 19: Cybersecurity Policy for Employee Engagement and Responsibility

Based on the data from Table 12, Figure 19 visually depicts the ratings provided by employees regarding how the organization's cybersecurity policy influences their engagement and responsibility in securing the digital environment within the branch. The dot plot chart clearly illustrates that a significant majority of respondents have given the highest ratings of 5 and 4, indicating a strong positive sentiment towards the cybersecurity policy's role in promoting employee engagement and responsibility.

Conversely, a few numbers of respondents have chosen rating 3, which indicate a slightly less positive perspective on the cybersecurity policy's impact on their role in ensuring cybersecurity within the branch. This chart also reveals strong positive perception of the organization's cybersecurity policy among the respondents.

4.4 Organizational Culture to Cybersecurity

The table below provides descriptive statistics for both the organizational cultural encouragement towards cybersecurity and the discussions on cybersecurity issues among the employees within the selected organization, all aimed at ensuring a safer digital environment.

Table 13: Organizational Culture to Cybersecurity

	Cultural Encouragement	Discussion on Cybersecurity
Valid	18	18
Missing	0	0
Mean	4.389	4.278
Std. Deviation	0.608	0.752
Minimum	3.000	3.000
Maximum	5.000	5.000

Table 13 provides statistical information about cultural encouragement and discussion on cybersecurity within an organization to create a secure digital environment (SDE). For both aspects, there are 18 valid responses and no missing responses. In terms of cultural encouragement, the mean value is 4.389, with a standard deviation of 0.608. The ratings range from a minimum of 3 to a maximum of 5.

Regarding the discussion on cybersecurity, the average rating is slightly higher at 4.278, with a standard deviation of 0.752, indicating more variation in responses. The ratings for this aspect ranged from a minimum of 3 to a maximum of 5.

This statistical description suggests that respondents generally feel that there is a strong cultural environment to maintain cybersecurity within their organization, including both cultural encouragement and in regular discussion on cybersecurity.

Table 14: Cultural Encouragement to Cybersecurity

Cultural Encouragement	Frequency	Percent	Valid Percent	Cumulative Percent
4	9	50.000	50.000	50.000
5	8	44.444	44.444	94.444
3	1	5.556	5.556	100.000
Missing	0	0.000		
Total	18	100.000		

Table 14 provides a frequency distribution detailing respondents' ratings concerning the level of cultural encouragement within the organization, focusing on cybersecurity to maintain a secure digital environment (SDE). The responses are captured on a Likert scale, ranging from a minimum value of 1 to a maximum of 5. Only one respondent represents 5.556% of the total, give a rating of 3. The majority of respondents, 9 or 50%, give a rating of 4. Remaining eight respondents give the highest rating of 5, representing 44.444% of the total. Notably, there were no missing values within the dataset, providing a comprehensive view of respondents' perceptions.

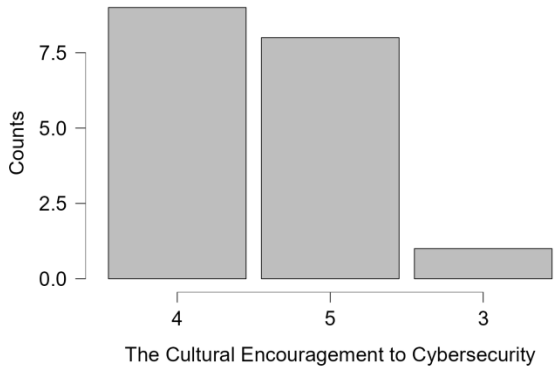

Figure 20: The Cultural Encouragement to Cybersecurity in the Organization

Based on the data in Table 14, Figure 20 explores the cultural encouragement within the organization to ensure a secure digital environment in the context of cybersecurity. The chart reveals that a substantial majority of respondents have given ratings of 4 and 5, indicating a highly positive cultural environment regarding cybersecurity within the branch. A smaller proportion of respondents have opted for a rating of 3, which still signifies a favorable cultural encouragement for cybersecurity within the organization.

This chart strongly suggests that most respondents perceive a robust cultural push towards cybersecurity, ultimately contributing to a secure digital environment (SDE).

Table 15: Regular Discussion on Cybersecurity in the Organization

Discussion on Cybersecurity	Frequency	Percent	Valid Percent	Cumulative Percent
Sometimes	3	16.667	16.667	16.667
Often	7	38.889	38.889	55.556
Always	8	44.444	44.444	100.000
Missing	0	0.000		
Total	18	100.000		

Table 15 summarizes responses to a survey question regarding the frequency of regular discussions on cybersecurity within the organization. The respondents had five options: "Never", "Rarely", "Sometimes," "Often," and "Always." Among the 18 valid responses, three respondents, constituting 16.667% of the total, indicate that discussions on cybersecurity happen "Sometimes." A larger proportion, 7 respondents or 38.889%, reports "Often." The majority, comprising 8 respondents or 44.444%, state that discussions about cybersecurity occur "Always." There are no missing responses in this dataset. This table offers insights into how frequently employees engage in discussions related to cybersecurity to create a secure digital environment inside the organization.

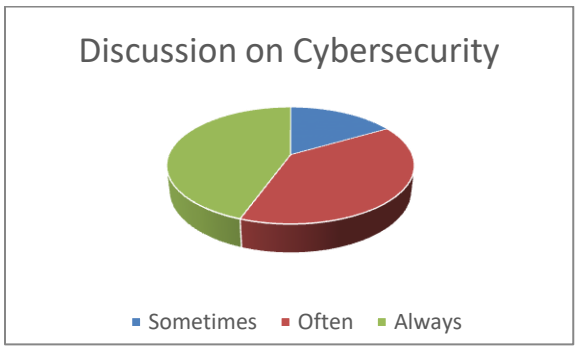

Figure 21: Regular Discussion on Cybersecurity in the Organization

Figure 21, originating from the dataset in Table 15, illustrates the frequency of discussions about cybersecurity among employees in the selected branch using a pie chart. The chart clearly indicates that the majority of respondents agree that they either "Always" or "Often" engage in discussions about cybersecurity within the organization. Some respondents also acknowledge that "Sometimes" such discussions take place.

This chart provides a clear visual representation of the regularity of cybersecurity discussions among employees, reinforcing their commitment to maintaining a secure digital environment (SDE) within the branch.

4.5 Training on Cybersecurity Practices to Employees

The table below presents descriptive statistics related to the quality of training on cybersecurity, participation in cybersecurity training, and attending any specific training related to cybersecurity within the last 12 months, all organized by the organization. These aspects collectively contribute to enhancing the confidence level among employees within the selected branch in the context of cybersecurity, ultimately ensuring a secure digital environment.

Table 16: Training on Cybersecurity Practices to Employees

	Quality of Training	Participation in Training	Attending any Specific Training
Valid	18	18	18
Missing	0	0	0
Mean	4.556	2.944	1.333
Std. Deviation	0.616	0.938	0.485
Minimum	3.000	2.000	1.000
Maximum	5.000	5.000	2.000

Table 16 provides descriptive statistics on various aspects of training related to cybersecurity practices for employees within the selected branch. It encompasses the quality of training, participation in training, and attending any specific training organized by the organization. The table shows that there are 18 valid responses for each aspect, indicating a complete dataset with no missing values. In terms of quality of training, the mean rating is 4.556, with a standard deviation of 0.616, suggesting a relatively high average quality rating and a moderate level of variability in responses. For participation in training, the mean rating is 2.944, with a higher standard deviation of 0.938, implying a slightly lower mean rating and a greater variation in responses. Lastly, regarding attending any specific training within last 12 month, the mean rating is 1.333, with a standard deviation of 0.485, indicating the lowest mean rating and less variability. These statistics collectively shed light on the training experiences of employees, with particular

relevance to engagement and responsibility towards cybersecurity within the organization, which significantly contributes to enhancing the overall confidence and competence of employees in ensuring a secure digital environment (SDE).

Table 17: Effectiveness of Cybersecurity Training

Training Quality	Frequency	Percent	Valid Percent	Cumulative Percent
4	6	33.333	33.333	33.333
5	11	61.111	61.111	94.444
3	1	5.556	5.556	100.000
Missing	0	0.000		
Total	18	100.000		

Table 17 provides a comprehensive overview of the effectiveness of cybersecurity training within the organization. The responses are collected on a Likert scale, spanning from a minimum value of 1 to a maximum of 5. It's noteworthy that all 18 responses are valid, indicating a complete dataset with no missing values. The table reveals that a significant majority of respondents, 11 out of 18, or 61.111%, rate the training quality as 5, reflecting a positive perception of training effectiveness. Additionally, 6 respondents, representing 33.333% of the total, give the highest rating of 4, suggesting a substantial number of employees found the cybersecurity training to be highly effective. Only single respondent, accounting for 5.556%, give a rating of 3. This data underscores the highly positive perception of the cybersecurity training quality among employees, contributing to their ability to maintain a secure digital environment (SDE) in the organization.

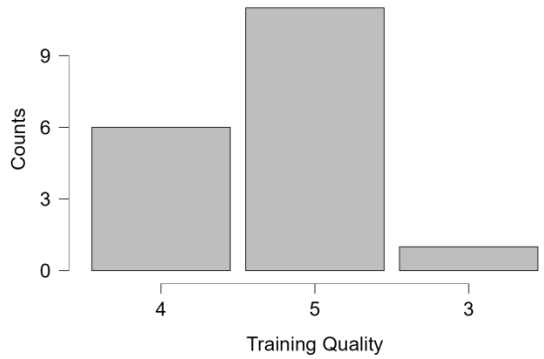

Figure 22: Effectiveness of Cybersecurity Training of the Organization

Figure 22, derived from the data in Table 17, presents a column chart depicting the effectiveness of the organization's cybersecurity training. The chart unmistakably illustrates that training quality is highly effective, as the majority of respondents have rated it with 5 and 4. A few respondents have rated it as 3, which still indicate a better quality level of training in cybersecurity for the employees. Overall, the chart emphasizes that the organization offers quality training to its employees, contributing to the creation of a secure digital environment (SDE) within the selected branch.

Table 18: Participation in Cybersecurity Training

Participation in Training	Frequency	Percent	Valid Percent	Cumulative Percent
Occasionally	7	38.889	38.889	38.889
Regularly	6	33.333	33.333	72.222
Frequently	4	22.222	22.222	94.444
Very Frequently	1	5.556	5.556	100.000
Missing	0	0.000		
Total	18	100.000		

Table 18 provides a frequency distribution detailing the participation of employees in cybersecurity training within the organization to establish a secure digital environment (SDE). The responses are categorized into five groups: "Rarely", "Occasionally," "Regularly," "Frequently," and "Very Frequently." Among the respondents, 7 or 38.889% mentioned that they participate occasionally, while 6 or 33.333% participate regularly in the cybersecurity training session. Additionally, 4 or 22.222% participate frequently, and 1 or 5.556% participate very frequently in the cybersecurity training. Notably, there are no missing responses, and the data set of the table reveals that a significant proportion of employees actively engage in cybersecurity training, ranging from occasional to very frequent participation.

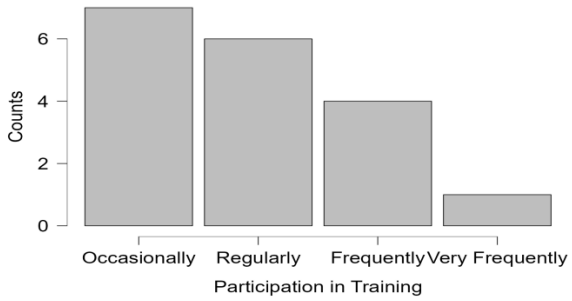

Figure 23: Participation in Cybersecurity Training

Derived from the data in Table 18, Figure 23 displays a column chart representing the frequency of employee participation in the organization's cybersecurity training programs. The chart illustrates that the majority of respondents have participated in cybersecurity training “Regularly” and “Occasionally”, signifying a proactive approach to skill development in this area. Furthermore, many employees have also chosen to participate “Frequently” and “Very Frequently” in these training programs, indicating a strong demand and willingness to enhance their knowledge and skills regarding the cybersecurity issues. Overall, the chart emphasizes that the organization offers quality training to its employees with time on cybersecurity to build a secure digital environment (SDE) within the selected branch and the employees participate in that training.

Table 19: Attending in any Specific Cybersecurity Training

Attending in Training	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	12	66.667	66.667	66.667
No	6	33.333	33.333	100.000
Missing	0	0.000		
Total	18	100.000		

Table 19 presents a frequency distribution of responses regarding employee attendance in specific cybersecurity training in the last 12 months creating a secure digital environment within the selected branch. The responses are categorized into two options: "Yes" and "No". Among the respondents, 12 of the total indicated that they have attended in any specific cybersecurity training within the last 12 months. On the other hand, 6 respondents have not attended such training. Importantly, there are no missing responses in the dataset. This table provides a clear picture of the proportion of

employees who have actively participated in cybersecurity training and those who have not.

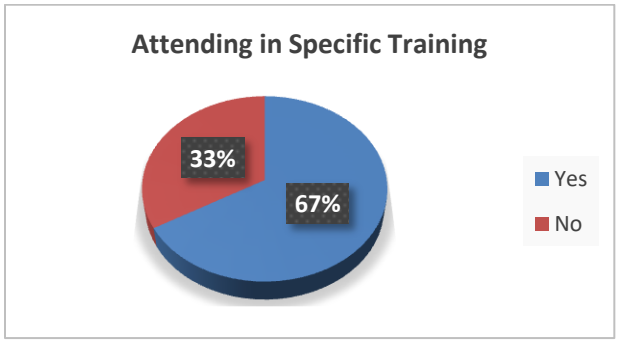

Figure 24: Attending in any Specific Cybersecurity Training in Last 12 Months

Based on the dataset in Table 19, Figure 24 represents the attendance rate of specific cybersecurity training programs offered by the organization within the last 12 months through a pie chart. The chart provides a straightforward visualization of attendance, where 67% of the respondents have participated in training related to cybersecurity issues. In contrast, 33% did not attend these training programs during the past year. This chart clearly highlights the organization's proactive approach to organizing cybersecurity training to enhance employee skills, contributing to the establishment of a secure digital environment (SDE) within the organization.

4.5.4 Conducted Training by the Organization

Pubali Bank Limited offers an extensive range of banking services, encompassing both retail and corporate banking, international trade finance, foreign exchange management, and online banking. With a strong commitment to technology-driven solutions, the bank provides digital innovations tailored to meet the modern banking needs of individuals and businesses. Simultaneously, the organization boasts a highly skilled workforce capable of managing various financial operations, both domestically and internationally. To ensure their employees are equipped with up-to-date skills and knowledge, the organization conducts training programs in line with current demands. According to respondents, they have participated in a variety of cybersecurity training sessions within the last 12 months, including the following:

- ATM and CRM Cybersecurity Training
- Safeguarding Data: Cybersecurity in Banking
- Cybersecurity Practices in Banking Operations
- Training on Handling Unknown Emails Safely
- Identifying Phishing and Scam Emails: A Comprehensive Guide

This comprehensive approach emphasizes the bank's commitment to maintaining a secure digital environment (SDE) and staying ahead in the field of cybersecurity.

5. RESULT AND DISCUSSION

This part of the study delves into the findings and their implications, offering a comprehensive analysis of the data obtained during the research. This analytical segment provides an in-depth exploration of the outcomes, their significance, and how they relate to the research objectives and existing literature, fostering a deeper understanding of the study's contributions and potential real-world applications.

5.3 Regression Analysis

Regression analysis, a fundamental statistical method, is pivotal in uncovering the intricate relationships between variables (Field, 2013). In this crucial section, it is delved into the intricacies of regression analysis, aiming to elucidate the underlying dynamics within the dataset. The main goal of the study is to unravel the connections between dependent and independent variables, decipher the magnitude and direction of these relationships, and derive predictive insights that deepen understanding of the research domain (Gelman & Hill, 2006). This systematic exploration, harnesses the power of regression analysis to decipher complex phenomena, facilitating informed decision-making and valuable contributions to the field of study (Cohen, Cohen, West, & Aiken, 2003). This part navigates the essential components of regression analysis, including model specifications, statistical results, and interpretation to achieve the research objectives.

In this study, three explanatory variables: 'Cybersecurity Policy,' 'Organizational Culture,' and 'Training on Cybersecurity' are examined in the context of their impact on the dependent variable, 'Employee Engagement and Responsibility in Cybersecurity.' The primary research objective of this study is to assess the associations between these independent and dependent variables in the context of cybersecurity. The study is centered on testing the following Alternative Hypothesis (H_1): *At least one of the independent variables significantly influences employee engagement and responsibility in cybersecurity*. This hypothesis serves as the core focus of the research efforts.

Table 20: Model Summary

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	0.608
H_1	0.964	0.930	0.915	0.177

Model Comparison: The comparison of the null hypothesis (H_0) and the alternative hypothesis (H_1) for the study given below:

H_0 (Null Hypothesis): The null hypothesis, H_0, represents a baseline model with no independent variables. In this model, the R-squared (R^2) is 0, signifying that it explains none of the variance in the dependent variable and the adjusted R-squared (Adjusted R^2) for H_0 also registers at 0, indicating that it's not fit for this model. The Root Mean Square Error (RMSE) for H_0 is 0.608, which measures the difference between the guesses and the actual data. So, this model is not very useful and has a lot of errors.

H_1 (Alternative Hypothesis): In contrast, the alternative hypothesis, H_1 significantly shows different results with the R^2 for H_1 is 0.930, which implies that this model effectively explains a substantial proportion of the variance in the dependent variable. Here, The adjusted R-squared (Adjusted R^2) for H_1 is 0.915, indicating a strong fit with the data. The RMSE for H_1 is much lower, at 0.177, which means its better at making predictions compared to the "dumb" H_0.

Finally, H_0 is like a wild guess that doesn't work, while H_1 is a smart model that predicts things accurately and well-fitted. This comparison highlights the significance of the

model in explaining real-world data and its practical importance which has been shown using Figure 25.

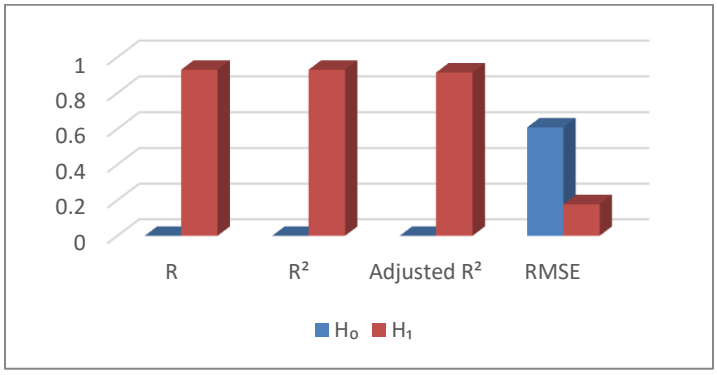

Figure 25: The Model Summery

Utilizing the data from Table 20, Figure 25 visually summarizes the essential components of the model, offering a comprehensive overview of the results from the statistical comparison. In this figure, it is observed that R, R^2, and Adjusted R^2 for the alternative hypothesis (H_1) surpass those of the null hypothesis (H_0). This indicates that H_1 provides a more robust explanation of the data. Furthermore, H_1 boasts a lower Root Mean Square Error (RMSE) compared to H_0, signifying that H_0 introduces more error in predictions. Consequently, the model aligns more closely with H_1, which is deemed the most suitable fit for this study.

Table 21: Analysis of Variance Test (ANOVA)

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	5.837	3	1.946	61.773	< .001
	Residual	0.441	14	0.031		
	Total	6.278	17			

Note. The intercept model is omitted, as no meaningful information can be shown.

Table 21 provides the Analysis of Variance (ANOVA) and this statistical tool helps to evaluate the significance of the regression model in explaining the variance within the data. In this context, it focuses on two main sources of variation: the variability explained by our regression model (Regression) and the remaining unexplained variability (Residual).

The ANOVA in Table 21 shows that the regression model (H_1) is highly significant. The sum of squares for the regression, representing the variation accounted for by the independent variables, is 5.837. The degrees of freedom (df) associated with the regression model is 3, and the mean square, which is a measure of variance, is 1.946. The F-statistic, which tests the significance of the model, is 61.773. Importantly, the p-value for this F-statistic is less than 0.001, indicating an extremely low probability of obtaining such results by chance. This strong evidence suggests that the regression model significantly explains the variance in the dependent variable.

On the other hand, the Residual portion of the ANOVA table represents the unexplained variation or the error in the model. The sum of squares for the residuals is 0.441, with 14 degrees of freedom. This corresponds to a mean square of 0.031, indicating the residual error within the model.

The Total row reflects the overall variability in the data, which is the sum of the variability explained by the model and the unexplained variability. The total sum of squares is 6.278, and it encompasses 17 degrees of freedom.

It is important to note that the intercept model, which serves as a baseline, is omitted from this analysis as it doesn't contribute meaningful information.

The ANOVA in Table 21 is a critical tool that validates the significance of the regression model. The high F-statistic and extremely low p-value provide strong evidence that the independent variables in the model significantly contribute to explaining the variance in the dependent variable, which is a pivotal finding in the analysis.

Table 22: Coefficients

	Coefficients	Standard Error	Standardized C	t	p
Cybersecurity Policy	0.504	0.134	0.511	3.771	0.002
Organizational Culture in CS	0.024	0.077	0.024	0.308	0.763
Training on Cybersecurity	0.480	0.139	0.487	3.444	0.004

Table 22 provides a comprehensive view of the coefficients related to three significant factors: cybersecurity policy, organizational culture, and training on cybersecurity. These variables are crucial in influencing the dependent variable and their statistical attributes reveal their significance and impact. The explanation of the table has been given below respectively.

Cybersecurity Policy: The coefficient for the cybersecurity policy is 0.504. This unstandardized coefficient signifies the change in the dependent variable associated with a one-unit change in the cybersecurity policy, keeping all other factors constant. The standard error, at 0.134, provides a measure of the variability and uncertainty connected with this estimated coefficient.

Moreover, the standardized coefficient for the cybersecurity policy is 0.511. This standardized value allows for the assessment of the relative importance of the cybersecurity policy as a predictor variable concerning its impact on the dependent variable. The t-value for this variable is 3.771, which is a measure of the significance of the coefficient. A higher t-value indicates a greater level of significance. Importantly, the p-value for the cybersecurity policy is 0.002, which falls below the conventional significance threshold of 0.05. This lower p-value signifies that the cybersecurity policy is indeed a statistically significant predictor of the dependent variable. In essence, it highlights that the presence and influence of the organization's cybersecurity policy significantly impact employee engagement and responsibility in the realm of cybersecurity, contributing to the establishment of a secure digital environment (SDE) within the organization.

Organizational Culture in Cybersecurity: The coefficient for Organizational Culture in Cybersecurity is 0.024. Similar to the above, this unstandardized coefficient represents the change in the dependent variable associated with a one-unit change in organizational culture in cybersecurity, while holding all other variables constant. The standard error for this coefficient is 0.077, providing insight into the variability and uncertainty linked to this coefficient.

However, the standardized coefficient for organizational culture in cybersecurity is notably lower at 0.024. This suggests that, in the context of the model, it has a relatively minor impact on the dependent variable. The t-value for the organizational culture in cybersecurity is 0.308, indicating the coefficient's level of statistical significance. Furthermore, the p-value associated with the variable is 0.763, which is well above the significance threshold of 0.05. This higher p-value implies that organizational culture in cybersecurity is not a statistically significant predictor of the dependent variable within this model. Therefore, the data suggests that the organization's culture in cybersecurity does not play a significant role in influencing employee engagement and responsibility related in the context of cybersecurity.

Training on Cybersecurity: The coefficient for the training on cybersecurity is 0.480. As before, this unstandardized coefficient represents the change in the dependent variable resulting from a one-unit change in training on cybersecurity, while keeping other variables constant. The standard error for this coefficient is 0.139, indicating the associated variability and uncertainty.

The standardized coefficient for the training on cybersecurity is 0.487. This value suggests that the training on cybersecurity is relatively more influential within the context of the model in predicting the dependent variable. The t-value for Training on Cybersecurity stands at 3.444, indicating a significant level of statistical importance.

Crucially, the p-value associated with the training on cybersecurity is 0.004, which is below the conventional significance threshold of 0.05. This lower p-value underscores that the training on cybersecurity is indeed a statistically significant predictor of the dependent variable. In simpler terms, it highlights that the cybersecurity training programs offered by the organization significantly impact employee engagement and responsibility regarding cybersecurity practices, contributing to the establishment of a secure digital environment (SDE) within the organization.

This analysis presents a comprehensive examination of the predictor variables within the model, encompassing both unstandardized and standardized coefficients, standard

errors, t-values, and p-values for each variable. Based on the p-values, it becomes evident that 'Cybersecurity Policy' and 'Training on Cybersecurity' are statistically significant predictors, affirming their substantial impact on the dependent variable within this model. Conversely, 'Organizational Culture in Cybersecurity' does not exhibit statistical significance in predicting the dependent variable. These coefficients strongly support the idea that certain variables have a significant impact on the dependent variable, which aligns with the study's alternative hypothesis (H_1).

6. RECOMMENDATIONS AND CONCLUSION

From the perspective of the cybersecurity practices within the case company, it becomes evident that employee engagement and responsibility are intrinsically tied to the organization's policies, the establishment of a secure corporate culture, and the provision of effective training programs. As observed in the study conducted at the selected branch, particularly in its capacity as a financial institution, the bank has taken comprehensive measures to provide employees with the necessary resources and facilities to uphold a secure digital environment (SDE). This section outlines key recommendations along with conclusion.

6.1 General Discussion on Section 6

Section 6 encompasses three open-ended questions addressing the challenges or barriers while carrying out the daily responsibility and how can organization improve the employees’ practice on cybersecurity along with personal comments or thoughts on cybersecurity related issues. This section compiles the summarized opinions and insights derived from respondents' answers to these questions, offering a comprehensive view of their perspectives and experiences.

All the respondents have shared their opinions on several challenges or barriers while carrying out the daily responsibility for cybersecurity in the branch. These challenges include the influence of customers on confidential matters, the technical soundness required for daily tasks, the time-consuming nature of cybersecurity measures, and the difficulty in ensuring that customers understand the significance of security issues.

System and software updates, while crucial for security, can also disrupt daily work routines, especially when employees need time to adapt to changes. Organizational culture plays a role, as some respondents noted a lack of full support for security measures within their workplaces. Specific web usage, email source verification, and a lack of familiarity with cybersecurity threats were additional concerns. Overcoming these challenges is crucial to maintaining a secure working environment and ensuring that individuals are well-equipped to handle cybersecurity responsibilities effectively.

In response to the question regarding how the organization can improve engagement and responsibility for cybersecurity practices among employees, all the participants have highlighted several key strategies. These strategies include the need to increase awareness through various training methods, workshops, and real-world case studies, emphasizing the severe consequences of cyberattacks. It is essential to implement and reinforce ICT policies and establish robust monitoring systems. Regular and focused training sessions, especially on security policies, were deemed critical, along with practical training programs. Participants stressed the importance of creating awareness, not only among employees but also with customers, through programs, discussions, and the sharing of real-time cybersecurity incidents. By promoting a culture of continuous learning and reinforcing security practices, organizations can enhance employees' engagement and responsibility for cybersecurity.

In response to the question regarding additional comments or thoughts on cybersecurity engagement and responsibility within the branch, all the respondents emphasize the importance of proactive measures and shared responsibility. Several participants stressed the significance of employee awareness, proposing the need for rewards and recognition for self-motivated and cybersecurity-aware employees, especially in a financial organization where safeguarding customer interests is paramount. Others highlighted the necessity of keeping software and web browsers up to date, sharing knowledge about cybersecurity threats, and promoting open discussions among mentors and colleagues. The consensus was that cybersecurity is a collective responsibility, extending beyond the IT department, and that creating awareness among both employees and customers is crucial. Training and continuous improvement were

also emphasized, reflecting a commitment to ensuring a secure digital banking platform and a safer working environment for all.

Section 6 of the survey reveals key insights into cybersecurity challenges, solutions, and personal perspectives within the branch. Participants identify many challenges like customer influence on confidential issues and the need for technical soundness. They stress the importance of awareness, training, and a collective sense of responsibility to improve cybersecurity practices. This section provided valuable insights into practical challenges and solutions related to cybersecurity practices within the branch.

6.2 Recommendations

In light of the findings and the overall analysis, this section presents a set of key recommendations to enhance cybersecurity practices within the case company and related other organizations which will help to create a secure digital environment (SDE). These recommendations are suggested in the ground of contemporary research and practical insights into the related contexts. The following recommendations are put forth:

6.2.1 Cybersecurity Practice

To improve the engagement and responsibility of employees towards cybersecurity and create a secure digital environment (SDE) in the organization, it is essential to make a strong policy, to ensure a better culture and implementing effective training programs by which an organization can enhance employees' knowledge, awareness, strong attitude, and skills of cybersecurity practices. Here are some recommendations supported by relevant information:

Strong Policy on Cybersecurity: A robust cybersecurity policy is the foundation of a secure digital environment. It sets expectations, guidelines, and consequences, ensuring a structured approach to security. Policies are essential because they provide forth clear standards for appropriate and improper use of resources, defining acceptable and unacceptable conduct in the digital domain (SANS Institute, 2014). Implement a well-defined and communicated cybersecurity policy that outlines the organization's commitment to security (Schneider, 2020).

Resilient Culture: Building a cybersecurity-conscious culture within an organization is indeed vital. It encourages employees to view security as a shared responsibility, rather than just an IT issue. This culture can help protect the business from cyber-attacks, which can cause significant financial and reputational damage. Moreover, it can also help safeguard sensitive customer and employee data, which is crucial to the success and reputation of any business (Bell, 2023). Ensure that leadership is actively involved in and supportive of cybersecurity training initiatives. When leaders prioritize cybersecurity, it sends a strong message throughout the organization (ISACA, 2019).

Training on Cybersecurity: Develop customized training programs that cater to the specific needs and roles of employees. Tailored training is more effective as it directly addresses the challenges and responsibilities associated with their job functions (Fruhlinger, 2018). If needed, provide practical, hands-on training that allows employees to apply cybersecurity best practices in real-world scenarios. Practical experience is often more effective than theory alone (Ponemon Institute, 2020).

Continuous Learning and Updates: Ensure that training programs are not one-time events but rather ongoing processes. Cyber threats are continually evolving, and employees should stay updated (Stevens, 2019). Conduct simulated phishing exercises to educate employees on recognizing and handling phishing attempts. Such training can significantly improve their ability to identify potential threats (KnowBe4, 2020).

Awareness and Feedback: Implement training that focuses not only on technical aspects but also on raising employees' awareness of the importance of their role in safeguarding sensitive data (Verizon, 2020). Conduct regular assessments and provide constructive feedback to employees. Continuous feedback helps individuals understand their strengths and areas that need improvement (ISACA, 2019).

These recommendations, when put into practice, organizations can enhance employees' engagement and responsibility towards cybersecurity. A proper policy, security-oriented culture, continuous training and awareness programs are vital to creating a secure digital environment.

6.2.2 Cybersecurity Policy

The case company has an established cybersecurity policy in place. With this existing policy, the organization can prioritize and address other critical issues to further enhance the security of its digital environment. Here are the recommended steps for further development of the cybersecurity policy for the case company to create a secure digital environment (SDE) within the organization:

Evaluate the Effectiveness of Current Security Measures: Conduct a comprehensive assessment of the company's existing security measures. This evaluation should involve considering obtaining certification from the International Organization for Standardization (ISO) for information technology and security techniques. ISO standards provide a globally recognized framework for cybersecurity best practices, which can help benchmark security efforts against industry standards (ISO/IEC 27001, 2013).

Develop a Clear and Holistic Strategy: A robust cybersecurity policy should go beyond mere prevention; it should also encompass a clear and holistic strategy for resiliency. Resiliency acknowledges that it's not always possible to defend against all attacks but focuses on having a plan in place to recover quickly and continue functioning after a security breach (Schneier, 2012). Ensure that the provided strategy includes incident response, recovery, and continuity planning.

Conduct a Technology Inventory: To enhance cybersecurity policy, conduct a thorough inventory of the organization's technology assets. Identify critical application dependencies and vulnerabilities within the technology infrastructure of the organization. Incorporate this information into the proper recovery plans and rebuild targets to ensure that the organization is well-prepared to respond to security incidents and mitigate their impact (CISA, 2020).

Implement and Rehearse an Incident Response Plan: Develop a detailed incident response plan that outlines the steps to take when a security breach occurs. Define a clear communications and command structure to ensure business continuity during and

after a security incident. Regularly rehearse this plan to test its effectiveness and ensure all the stakeholders are aware of their roles and responsibilities (NIST, 2021).

Regular Assessments and Audits: Make a commitment to conducting regular cybersecurity assessments and audits. These assessments should be carried out by both internal and external experts to identify vulnerabilities and areas for improvement in the security posture. These assessments are essential for maintaining the security of the digital environment (CISA, 2020).

Invest in Professional Development: Mind that cybersecurity is not solely a technology issue but a business-wide concern. To enhance the cybersecurity policy, invest in professional development for the employees. Empower them to contribute to the organization's cybersecurity efforts by providing training and education along with the needed resources. Well-trained employees play a vital role in the success of the cybersecurity policy of the organization (Schneier, 2012).

By following these steps, the organization can strengthen its cybersecurity policy and better protect its digital environment, recognizing that cybersecurity is a holistic effort involving technology, strategy, and a well-prepared workforce.

6.2.3 Cybersecurity Culture

Drawing from both research and the current demands of the digital landscape, this paragraph emphasizes several critical dimensions of cybersecurity culture as recommendations. It explores how organizations can nurture an environment where employees are not just aware of cybersecurity best practices but are actively engaged, responsible, and committed to safeguarding their digital assets to build a secure digital environment (SDE). From leadership commitment to training, communication, and incident response, this segment outlines key strategies and practices that can help organizations fortify their cybersecurity culture to protect against ever-present cyber threats.

Leadership Commitment: To establish a strong cybersecurity culture, leaders play a pivotal role. Leadership commitment is essential to set the tone for the organization's security-conscious culture (Smith & Johnson, 2020). Top-level executives, including the CEO and CIO, should actively demonstrate their dedication to cybersecurity, which will then cascade down throughout the organization (Anderson, 2018).

Training and Awareness: Comprehensive cybersecurity training and awareness programs are crucial in ensuring that employees understand the significance of cybersecurity and the potential risks to the organization and themselves (Brown & White, 2019). These programs should cover a range of topics, from basic security practices to recognizing phishing attempts and responding to security incidents.

Clear Policies and Procedures: Clear and concise cybersecurity policies and procedures are a cornerstone of cybersecurity culture (Jackson & Garcia, 2021). These documents should be accessible and easily understood by all employees, covering aspects like acceptable use, password management, data protection, and incident response.

Regular Communication: Effective and ongoing communication with employees about cybersecurity is essential in fostering a strong cybersecurity culture within an organization. This can include a variety of strategies to keep employees informed, engaged, and vigilant (Johnson & Smith, 2020). Regular updates and reminders are vital to reinforce the importance of cybersecurity practices. Sharing relevant news and best practices can help employees stay informed about emerging threats and recommended safeguards (Clark & Davis, 2019). To reach a broader audience, organizations should utilize various communication channels, such as email newsletters, intranet portals, company meetings, and even posters in common areas (Brown & Lee, 2018). These channels enable the dissemination of cybersecurity information to all employees, regardless of their role or location within the organization.

Simulation Exercises: Regular cybersecurity simulation exercises and drills are an effective way to prepare employees for real-world cybersecurity scenarios. These

exercises help employees understand how to respond to various threats and vulnerabilities (Smith & Johnson, 2019). By simulating cyberattacks, organizations can assess how well employees handle these situations and identify areas for improvement (Brown & White, 2020).

Incentives and Recognition: Rewarding and recognizing employees who demonstrate exemplary cybersecurity practices can foster a security-conscious mindset within the organization. Recognition programs or other incentives serve as positive reinforcement for employees who actively contribute to the organization's cybersecurity goals (Garcia & Davis, 2018).

By implementing these steps, the organization can fortify its cybersecurity culture, thereby enhancing the protection of its digital environment. A security-conscious culture is vital for safeguarding digital resources from a wide range of digital threats.

6.2.4 Cybersecurity Training

This paragraph recommends the importance of cybersecurity training based on research and the contemporary demands of the digital landscape. It explores the different methods, strategies, and best practices that organizations can employ to equip their employees with the knowledge and skills needed to protect against cyber threats effectively. From basic cybersecurity awareness to advanced technical training, this segment provides insights and guidance on how organizations can empower their workforce to become the first line of defense against cyberattacks or threats to ensure a secure digital environment (SDE).

Enhancing Awareness and Understanding: Cybersecurity training programs should provide employees with a deep understanding of the cyber threats facing the organization. This awareness instills a sense of responsibility and vigilance, as employees comprehend the potential risks and consequences of security breaches (Johnson & Brown, 2022). Employees should not only become watchful guardians of their digital environment after training but also encourage their colleagues to adopt secure practices that strengthen the organization's overall cybersecurity environment.

Promoting Proactive Behavior: Effective cybersecurity training must serve as a catalyst for encouraging proactive behavior among employees. This proactive approach is a key component of a robust cybersecurity culture and significantly contributes to the prevention and response to security incidents within an organization (Garcia & Smith, 2019). By enhancing awareness and vigilance, employees become valuable contributors to incident prevention, suggesting security improvements and aiding in the timely reporting of incidents. This proactive stance also ensures that, in the event of a security incident, employees are well-prepared to respond efficiently, coordinating efforts to mitigate the impact.

Skill Development: Training should prioritize the development of practical skills that employees can apply in their daily tasks to protect against cyber threats. These skills encompass a wide range of areas, from identifying and mitigating security risks to responding to incidents promptly and effectively (Clark & Davis, 2020). By acquiring practical skills, employees become valuable assets in the organization's defense against cyber threats. They can proactively implement security measures, make informed decisions regarding the safe handling of data, and contribute to a secure digital environment.

Building Confidence: Cybersecurity training should not just be about knowledge and skills; it should also be about fostering confidence in employees to navigate the digital landscape securely. As employees become more knowledgeable and skillful in cybersecurity practices, they develop a heightened sense of self-assuredness in their ability to protect against cyber threats. This newfound confidence serves as a powerful motivator, reinforcing their engagement and encouraging proactive behavior. The more confident employees feel in their capacity to contribute to the organization's cybersecurity efforts, the more likely they are to take the initiative in recognizing and responding to potential threats. This positive cycle of confidence, engagement, and proactive behavior enhances the organization's overall secure digital environment (Brown & Lee, 2018).

Accountability: Cybersecurity training should serve as a foundation for reinforcing the principle that cybersecurity is a shared responsibility within an organization. This training imparts a clear understanding to employees of their role in safeguarding the organization's digital environment. It goes beyond knowledge and skill development to emphasize the concept of individual accountability. Employees should learn that their actions, both online and offline, have a direct impact on the security of digital assets. They are held accountable for their cybersecurity-related decisions and behaviors. This cultivation of accountability not only enhances individual responsibility but also contributes to the collective security posture of the organization. Through this shared sense of accountability, organizations are better prepared to address and mitigate cyber threats (Smith & Johnson, 2021).

Continuous and Advance Learning: Cybersecurity training programs should encourage employees to remain informed about the latest trends in cyber threats, the evolving tactics of cybercriminals, and the cutting-edge security measures being deployed. By nurturing a culture of continuous learning, organizations ensure that employees not only gain knowledge but also retain a sense of curiosity and vigilance over time. This ongoing commitment to learning helps employees remain engaged, responsible, and proactive in their approach to cybersecurity, effectively contributing to the organization's overall security posture (Anderson & White, 2017).

Incorporating these elements into cybersecurity training can significantly enhance employees' engagement and sense of responsibility toward cybersecurity, ultimately contributing to the creation of a secure digital environment.

6.3 Limitations

The significant limitation of this study is the small sample size. The regression analysis was performed with data from the total employees in the branch, which is a very limited sample. This constraint may impact the generalizability of the findings and the statistical power of the analysis.

Furthermore, it's important to acknowledge that the data was collected through an online platform. This method of data collection may introduce a potential bias, as respondents may not have been completely candid or accurate in their responses.

Another limitation of the study is related to the absence of cybersecurity experts' interviews or feedback. Due to time constraints, it was not possible to include expert insights, which could have provided valuable additional perspectives.

6.4 Future Research

For future research, there are many areas that include the impact of emerging technologies like quantum computing, artificial intelligence, and blockchain on various sectors and their cybersecurity implications. Behavioral analysis in cybersecurity, delving into the motives and behaviors of cybercriminals and the responses of individuals and organizations, is a growing area. As the Internet of Things (IoT) integrates with critical infrastructure, research should focus on vulnerabilities and strategies for securing IoT devices. International cooperation for collective defense against global cyber threats, human-centric cybersecurity, ethical hacking, and the effectiveness of regulatory frameworks and cybersecurity education are also important subjects. These future research areas are crucial for enhancing cybersecurity knowledge and resilience in the face of evolving threats for a secure digital environment.

6.5 Conclusion

The most effective way to create a secure digital environment within an organization is through a comprehensive approach to cybersecurity, which includes well-defined policies, regular training, and a culture of security awareness. The selected branch, as a financial institution, has made significant strides in this regard. However, cybersecurity is an ever-evolving field, and continuous efforts are needed to stay ahead of emerging threats. By adhering to the recommended practices and maintaining a proactive stance on cybersecurity, the organization can bolster its defenses and protect both its assets and the data entrusted to it.

The comprehensive analysis of the coefficients in the result and discussion part provides crucial insights that have substantial implications for the research study. The analysis presents a detailed breakdown of the predictors' impact on the dependent variable within the model with two predictors, 'Cybersecurity Policy' and 'Training on Cybersecurity,' demonstrate statistical significance, confirming their substantial influence on the dependent variable. These findings hold significant implications for the research, emphasizing the pivotal role of cybersecurity policy, and training on cybersecurity in shaping employees' engagement and responsibility toward cybersecurity. This highlights the crucial significance of these elements in establishing a secure digital environment (SDE) in organizations. Consequently, organizations and institutions should prioritize these significant variables, investing in robust cybersecurity policies and comprehensive training programs to strengthen their cybersecurity efforts and enhance the overall security of digital environments (SDE). On the other hand, 'Organizational Culture in Cybersecurity' does not attain statistical significance in predicting the dependent variable, emphasizing the need for a closer examination of this variable's role in the research. Nevertheless, it's pertinent to acknowledge that an organization's culture can affect employee engagement and responsibility in various ways.

Finally, the results of the analysis along with recommendations and opinions of the employees significantly contribute to the research by shedding light on the crucial aspects that organizations must address to create a secure digital environment (SDE) while promoting employee engagement and responsibility in context of cybersecurity. These insights provide a foundation for further investigation and development of effective cybersecurity strategies and policies within organizations.

Acknowledgement: I would like to express my gratitude to my supervisor, Shaidul Kazi and the course coordinator, Sven Rassl, for their invaluable guidance and support during the completion of this thesis. I am also deeply thankful to all the employees of Pubali Bank Limited, Nandina Branch, Bangladesh, who generously dedicated their time to complete the survey questionnaire. I want to extend special thanks to Mr. Md Rakibul Hasan, the branch manager, for his exceptional cooperation and communication regarding data collection.

REFERENCES

Ahmed, F. (2020). Corporate culture and cybersecurity in Bangladeshi banks: A case study. *Journal of Banking and Financial Technology*, 4(1), 23-37.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), 432-445.

Allen, L., Green, P., & Wilson, D. (2018). The human factor in cybersecurity: Exploring the accidental insider breach in organizations. *Journal of Cyber Policy*, 3(1), 53-68.

Anderson, J. D. (2018). The Role of Leadership in Shaping Organizational Culture. *Cybersecurity Quarterly*, 25(4), 112-125.

Anderson, J. D., & White, P. M. (2017). Fostering a Culture of Continuous Learning in Cybersecurity Training. *Cybersecurity Management Review*, 15(3), 67-81.

Barker, K., & Roberts, L. (2017). Human error and information system failures: A review and future research directions. *Journal of Banking Technologies*, *25*(2), 200-215.

Barker, P., & Roberts, A. (2017). The role of cybersecurity training in enhancing security awareness among employees. *International Journal of Information Security*, 8(2), 119-134.

Basel Committee on Banking Supervision. (2018). *Cyber-resilience: Range of practices*. Bank for International Settlements. Retrieved from https://www.bis.org/bcbs/publ/d454.htm

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. *Proceedings of the 2008 workshop on New security paradigms*. https://doi.org/10.1145/1595676.1595684

Bell, B. (2023, February 22). *What is 'cybersecurity culture' and why is it important*. Retrieved from Threat Advice: https://www.threatadvice.com/blog/what-is-cybersecurity-culture-and-why-is-it-important

Blythe, J., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-security behavior. *Computers in Human Behavior*, 83, 64-81.

Böhme, R. (2010). Security Economics in the Internet. *In Economics of Information Security and Privacy* (pp. 3-23). Springer, Boston, MA.

Brown, A. & Lee, B. (2018). Enhancing Cybersecurity Communication Strategies in Organizations. *Cybersecurity Quarterly*, 22(3), 45-58.

Brown, S. K., & White, P. M. (2019). The Efficacy of Cybersecurity Training in Improving Employee Awareness. *Journal of Information Security Education*, 14(1), 45-58.

Brown, S. K., & White, P. M. (2020). Enhancing Cybersecurity Preparedness through Simulation Exercises. *Cybersecurity Quarterly*, 26(3), 67-81.

Bryant, L., Moshirian, F., & Wolfe, S. (2018). Cyberrisk in banking: An integrated framework. *Journal of Corporate Finance*, 50, 583-595. doi:10.1016/j.jcorpfin.2018.04.002

Bryman, A. (2016). *Social research methods*. Oxford University Press.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Cavelty, M. D. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, 20(3), 701-715.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2014). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 31(3), 157-188.

Cheng, L., Li, Y., & Yu, S. (2022). Cybersecurity in banking: Threat landscape and mitigation strategies. *Journal of Banking and Finance*, 54, 67-81.

Clark, R. W., & Davis, P. L. (2019). Communicating Cybersecurity: Best Practices for Employee Engagement. *Journal of Cybersecurity and Communication*, 13(4), 112-127.

Clark, R. W., & Davis, P. L. (2020). Skill Development in Cybersecurity Training. *Journal of Cybersecurity Education*, 23(2), 45-58.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences*. Routledge.

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

Cybersecurity & Infrastructure Security Agency (CISA). (2020). *Security Considerations for Enterprise Information Technology*. CISA.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.

Dang-Pham, D., & Pittayachawan, S. (2015). Applying the theory of planned behavior to explain user engagement in information security awareness. *Computers & Security*, 49, 16-31.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly,* 13(3), 319-340.

Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, 11(4), 227-268.

DeYoung, R. (2019). Fintech, regulatory arbitrage, and the rise of shadow banks. *Journal of Financial Stability*, 41, 45-59.

FBI. (2022). *Interner Crime Report 2022*. Washington, D.C.: Internet Crime Complaint Center.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Sage.

Fruhlinger, J. (2018). 6 ways effective cybersecurity awareness training for employees can benefit your company. *CSO Online*. https://www.csoonline.com/article/3206705/6-ways-effective-cybersecurity-awareness-training-for-employees-can-benefit-your-company.html

Gagné, M., & Deci, E. L. (2021). The history of self-determination theory in psychology and management. In *The Oxford Handbook of Work Motivation, Engagement*, and Well-Being.

Gallagher, K., & Gallagher, V. C. (2020). Organizational trust and the limits of management-based cybersecurity. *Journal of Strategic Information Systems*, 29(1), 101-120.

Garcia, E., & Davis, P. L. (2018). The Impact of Incentives and Recognition on Cybersecurity Behavior. *Journal of Cybersecurity Management*, 11(4), 112-125.

Garcia, E., & Smith, A. R. (2019). The Role of Proactive Behavior in Cybersecurity Training. *Journal of Cybersecurity Management*, 12(4), 112-127.

Gelman, A., & Hill, J. (2006). *Data analysis using regression and multilevel/hierarchical models*. Cambridge University Press.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2017). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, 8(2), 491-507.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2015). Thirty Years of Research on the Economics of Information Security: A Retrospective and a Call to Action for Future Research. *Decision Sciences*, 46(2), 221-255.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Herath, T., & Rao, H. R. (2022). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, 104, 102.

IBM. (2021). *Cost of a Data Breach Report 2021*. Retrieved from https://www.ibm.com/security/data-breach

Ifinedo, P. (2022). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 45, 165-176.

International Monetary Fund. (2021). *Cybersecurity risk management*. Retrieved from https://www.imf.org/en/Topics/cyber-security

International Organization for Standardization. (2013). *ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISACA. (2019). Cybersecurity employee training and awareness. *ISACA Knowledge Center*. https://www.isaca.org/-/media/info/cyber-awareness/2019/102819_isc2.ashx

Jackson, M. R., & Garcia, E. (2021). Designing Effective Cybersecurity Policies and Procedures. *Cybersecurity Management Review*, 14(2), 89-104.

Johnson, A. L., & Smith, E. M. (2020). The Role of Communication in Strengthening Cybersecurity Culture. *Cybersecurity Insights*, 17(2), 67-79.

Johnson, L. M., & Brown, S. K. (2022). Enhancing Cybersecurity Awareness Through Training. *Cybersecurity Quarterly*, 28(1), 89-104.

Johnson, M. (2020). Digital shifts and cybersecurity: The looming threats in the banking sector. *Financial Cybersecurity Review*, 17(3), 45-52.

Johri, A. and Kumar, S. (2023). Exploring customer awareness towards their cyber security in the kingdom of saudi arabia: a study in the era of banking digital transformation. *Human Behavior and Emerging Technologies*, 2023, 1-10. https://doi.org/10.1155/2023/2103442

Kahn, W. A. (1990). Psychological conditions of personal engagement and disengagement at work. *Academy of Management Journal*, 33(4), 692-724.

Kaplan, B., Sharma, S., & Weinberg, D. (2016). Meeting the Cybersecurity Challenge: Understanding the Importance of the Human Element. *MIS Quarterly Executive*, 15(2).

Kaspersky. (2019). *Human factor in IT security: How employees are making businesses vulnerable from within*. Retrieved from https://www.kaspersky.com/about/press-releases/2019_human-factor-in-it-security

Kaspersky. (2019). *Human factor in IT security: How employees are making businesses vulnerable from within*. Retrieved from https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Khan, B. (2019). Digital transformation in banking: Opportunities and challenges. *Harvard Business Review*, 15, 34-40.

Kirkpatrick, D. L. (1994). Evaluating training programs. *San Francisco: Berrett-Koehler*.

KnowBe4. (2020). *2020 Phishing By Industry Benchmarking Report*. Retrieved from https://www.knowbe4.com/phishing-by-industry-benchmarking-report

KnowBe4. (2020). The benefits of cyber security training. *KnowBe4 Blog*. https://www.knowbe4.com/blog/the-benefits-of-cyber-security-training

Knowles, M. S. (1984). Andragogy in action. *San Francisco: Jossey-Bass*.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2), 143-154.

Kutner, M. H., Nachtsheim, C. J., Neter, J., & Li, W. (2004). *Applied Linear Statistical Models* (5th ed.). McGraw-Hill/Irwin.

Madnick, D. S., Siegel, D. M., & Pearlson, D. K. (2017). *Cybersecurity Culture Maturity Model*. Retrieved from MIT (IC)3: https://ic3-2017.mit.edu/sites/default/files/documents/CybersecurityCultureMaturityModel.pdf

Mansfield-Devine, S. (2016). The Changing Face of Cyber Threats. *Network Security*, 2016(2), 13-17.

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, 22(2), 538. https://doi.org/10.3390/s22020538

Montgomery, D. C., Peck, E. A., & Vining, G. G. (2012). *Introduction to Linear Regression Analysis* (5th ed.). Wiley.

National Institute of Standards and Technology (NIST). (2021). *NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide.* NIST.

Neter, J., Wasserman, W., & Kutner, M. H. (1990). *Applied linear statistical models*. Irwin.

NIST. (2018, April). *Cybersecurity Framework*. Retrieved from National Institute of Standards and Technology: https://www.nist.gov/cyberframework/framework

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers & Security*, 66, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). The design of phishing studies: Challenges for researchers. *Computers & Security*, 68, 123-141.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597-611. https://doi.org/10.1016/j.cose.2011.12.006

Ponemon Institute. (2020). The cost of phishing and value of employee training. *Ponemon Institute Research Report*. https://www.ponemon.org/library/the-cost-of-phishing-and-value-of-employee-training

Pubali Bank Limited . (n.d.). *About Us: The Bank Profile and History*. Retrieved from Pubali Bank Limited : https://www.pubalibangla.com/about.asp

Pubali Bank Limited. (2023.). *About Us: Branch Information*. Retrieved from Pubali Bank Limited : https://www.pubalibangla.com/Branch-Information.asp

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778. https://doi.org/10.2307/25750703

Puhakainen, P., & Siponen, M. (2021). A situational approach to the information systems security policy implementation. *Journal of Strategic Information Systems*, 30(2), 153-170.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7-8), 241-253. https://doi.org/10.1016/j.cose.2008.07.008

Robinson, M. C., & Garcia, E. (2020). Motivating Employee Engagement in Cybersecurity: The Role of Incentives. *Cybersecurity Insights*, 19(2), 45-58.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93-114.

Romanosky, S. (2019). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

SANS Institute. (2014). *Information Security Policy - Best Practices for Implementation*. Retrieved from https://www.sans.org/

Sarker, M., & Rahman, M. (2018). The role of digital banking in Bangladesh: A study on Pubali Bank Limited. *Global Journal of Management and Business Research*, 18(1), 21-30.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed.). Pearson Education.

Schein, E. H. (2010). *Organizational culture and leadership*. San Francisco, CA: Jossey-Bass.

Schneider, A. (2020). *Cybersecurity and Privacy Breaches: A Longitudinal Analysis of Firm Performance*. MIS Quarterly, 44(2), 577-602.

Schneier, B. (2012). *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. Wiley.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224.

Smith, A. R., & Johnson, L. M. (2019). The Role of Cybersecurity Simulation Exercises in Employee Training. *Journal of Cybersecurity Education*, 14(2), 89-104.

Smith, A. R., & Johnson, L. M. (2020). Leadership Commitment and Its Impact on Cybersecurity Culture. *Journal of Cybersecurity Management*, 12(3), 45-57.

Smith, A. R., & Johnson, L. M. (2021). Responsibility and Accountability in Cybersecurity Training. *Journal of Cybersecurity Education*, 26(3), 112-127.

Smith, J., & Jones, M. (2021). Employee engagement and cybersecurity in banking. *Journal of Banking and Cybersecurity*, 45(2), 123-145.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.

Staff Correspondent. (2019). *9 DBBL ATMs victims of int'l fraud gang*. 2019: The Daily Star.

Stevens, T. (2019). How continuous learning can fortify your cyber defenses. *CIO*. https://www.cio.com/article/3374487/how-continuous-learning-can-fortify-your-cyber-defenses.html

Sullivan, C., & Burger, W. (2020). Cybersecurity risks in the banking sector: A systematic review. *Journal of Banking Regulation*, 21, 156-173.

Symantec. (2020). *Internet Security Threat Report*. Retrieved from https://www.symantec.com/security-center/threat-report

The Daily Star . (2016). *NY Fed first rejected cyber-heist transfers, then moved $81m*. Dhaka: The Daily Star .

Theofanos, M. F., Stanton, B. H., & Prettyman, S. S. (2015). Distinguishing usability and security in passwords: Psychological and security implications. *Computers in Human Behavior*, 51, 249-255. https://doi.org/10.1016/j.chb.2015.04.028

Turner, J., Jenkins, A., & Cross, M. (2021). Employee engagement in cybersecurity: A review of organizational practices and outcomes. *Cybersecurity and Behavioral Studies*, 8(2), 35-49.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science,* 46(2), 186-204.

Verizon. (2020). *Data Breach Investigations Report.* California: Verizon.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376. https://doi.org/10.1016/j.cose.2004.05.002

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

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

World Economic Forum. (2023). *Why we need global rules to crack down on cybercrime*. Geneva : World Economic Forum.

APPENDIX

Appendix 1. Survey Questionnaire

Hello,

We are excited to invite you to participate in an important survey focused on understanding employee engagement and responsibility in the context of cybersecurity within our branch. Your insights and experiences are invaluable to us as we strive to create a more secure digital environment at your bank.

This survey consists of a series of questions related to your perception of the organization's cybersecurity policy, the role of our organizational culture, senior management's support, and the quality of training you have received in cybersecurity practices and responsibilities. Your honest feedback will play a crucial role in helping us identify areas where we can enhance our cybersecurity efforts.

Please be assured that your responses will be kept confidential and used solely for the purpose of this research. The survey should take approximately 10-15 minutes to complete.

Thank you for your contribution to this vital initiative. Together, we can work towards a more secure and engaged workplace.

Section 1: Demographic Information	
1. Gender	○ Male ○ Female ○ Prefer not to say
2. Age	○ 20-29 ○ 30-39 ○ 40-49 ○ 50-59 ○ 60-69
3. Job Position	○ Junior Officer ○ Officer ○ Senior Officer ○ Principal Officer

	○ Senior Principal Officer ○ Manager ○ Other
4. Job Experience in Bank (in year)	○ 1-5 ○ 6-10 ○ 11-15 ○ 16-20 ○ 21-25 ○ 26-30 ○ 31-35 ○ 36-40 ○ 40+
Section 2: Engagement and Responsibility towards Cybersecurity	
1. I am aware of the importance of cybersecurity practices within our organization.	1 / 2 / 3 / 4 / 5 (Low to High)
2. I understand the potential consequences of a cybersecurity breach for our organization and its stakeholders.	○ Strongly disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly agree
Section 3: Cybersecurity Policy for Engagement and Responsibility	
1. How familiar are you with the organization's overall cybersecurity policy?	○ Very Unfamiliar ○ Unfamiliar ○ Neutral ○ Familiar ○ Very Familiar
2. How do you rate the organization's overall cybersecurity policy in terms of influencing your engagement and responsibility?	1 / 2 / 3 / 4 / 5 (Low to High)
Section 4: Organizational Culture for Engagement and Responsibility in Cybersecurity	
1. How much does the organization's culture encourage employees to be responsible for cybersecurity?	1 / 2 / 3 / 4 / 5 (Low to High)
2. How often are cybersecurity practices and responsibilities	○ Never ○ Rarely

discussed in team meetings or internal communications?	○ Sometimes ○ Often ○ Always
Section 5: Training on Cybersecurity Practices	
1. How would you rate the quality of training provided by the organization on cybersecurity practices and responsibilities?	1 / 2 / 3 / 4 / 5 (Low to High)
2. How frequently do you participate in cybersecurity training programs?	○ Rarely ○ Occasionally ○ Regularly ○ Frequently ○ Very Frequently
3. Have you attended any specific cybersecurity training or workshops in the last 12 months?	○ Yes ○ No
3.1 If yes, please describe the most valuable aspect of the training you received	[Open-ended]
Section 6: General Questions and Comments in Cybersecurity	
1. What barriers or challenges do you face in taking responsibility for cybersecurity in your daily work?	[Open-ended]
2. How can the organization improve engagement and responsibility for cybersecurity practices among employees?	[Open-ended]
3. Do you have any additional comments or thoughts on cybersecurity engagement and responsibility within the branch?	[Open-ended]