YANGON UNIVERSITY OF ECONOMICS

DEPARTMENT OF COMMERCE

MASTER OF BANKING AND FINANCE PROGRAMME

CYBER SECURITY TRAINING PRACTICES AND EMPLOYEE WORK PERFORMANCE AT GLOBAL TREASURE BANK

HNIN YU WAI

ROLL NO. 20

MBF 4th BATCH

JUNE, 2024

CYBER SECURITY TRAINING PRACTICES AND EMPLOYEE WORK PERFORMANCE AT GLOBAL TREASURE BANK

"This Thesis is submitted to the Board of Examiners in partial fulfillment of the requirements for the degree of Master of Banking and Finance (MBF)"

Supervised by:	**Submitted by:**
Dr. Thynn Thynn Myint	Hnin Yu Wai
Professor/Head	Roll No. 20
Department of Commerce	MBF 4th Batch
Yangon University of Economics	

JUNE, 2024

ACCEPTANCE

Accepted by the Board of Examiners of the Department of Commerce, Yangon University of Economics, in partial fulfillment for the requirements of the Master Degree, Master of Banking and Finance.

BOARD OF EXAMINERS

……………………….

Prof. Dr. Tin Tin Htwe
(Chairperson)
Rector
Yangon University of Economics

…………………………………

(Supervisor)
Prof. Dr. Thynn Thynn Myint
Professor/Head
Department of Commerce
Yangon University of Economics

…………………………………

(Examiner)
Prof. Dr. Aye Thanda Soe
Professor
Department of Commerce
Yangon University of Economics

…………………………………

(Examiner)
Prof. Dr. May Su Myat Htway Aung
Professor
Department of Commerce
Yangon University of Economics

…………………………………

(Examiner)
Dr. Phu Pwint Nyo Win Aung
Associate Professor
Department of Commerce
Yangon University of Economics

JUNE, 2024

ABSTRACT

This study investigates the relationship between cybersecurity training practices and employee work performance at Global Treasure Bank (GTB), emphasizing the impact on organizational cybersecurity strength in the digital financial landscape. The research employs a quantitative approach, utilizing structured questionnaires distributed among 150 IT managers and staff across 150 branches in Myanmar, using a five-point Likert scale. The data is used to analyze the relationships between the independent and dependent variables. The training needs, the training objective, the training content, the training methods, and the training evaluation are considered independent variables; the employee behavior and employee work performance considered a dependent variable. Regression analysis exposed a positive and significant relationship between employee job performance and selected cyber security training practices, except for training methods in GTB Bank. Additionally, it has been found that cybersecurity training techniques have the most significant impact on employee work performance. The results of this study the need for financial institutions to invest in robust, ongoing training programs tailored to the specific challenges of the cybersecurity landscape. By doing so, banks like GTB can enhance their resilience against cyber threats, ensuring the protection of their assets and maintaining the trust and confidence of their customers.

ACKNOWLEDGEMENTS

After completing this research paper, I would like to express my heartfelt gratitude to everyone who participated and helped me in various ways before, during, and after the study's preparation.

First and foremost, I would like to express special thanks and gratitude to Professor Dr. Tin Tin Htwe, Rector of the Yangon University of Economics, for her generous opportunity to participate in this Master of Banking and Finance Program.

Secondly, my heartfelt wish to extend my special thanks to Professor Dr. Thynn Thynn Myint, Head of Department of Commerce and Director of Master of Banking and Finance Programme, Yangon University of Economics for her valuable guidance and comment to accomplish this thesis. In addition, her great support and motivational guidance, many thanks for her constructive advice and supervision, which contributed helpful suggestions in the preparation of this paper.

Thirdly, my I also wish to express my respectful and thankful to my great appreciation to Professor Dr. Tin Tin Htwe former programme director from Department of Commerce, Yangon University of Economics for her great support, inspiring guidance, constructive counseling throughout my studies. Moreover, I would like to express my respectful gratitude to all teachers and lecturers for valuable knowledge and lectures during this course.

In addition, my special deepest thanks to the management team, the Learning and Development Department, and all GTB Bank respondents in my organization for their honesty, participation, and supervision, which enabled this study to be completed. Without their support for providing data and information.

Finally, I am very grateful to my family for their encouragement and all teachers for their valuable lectures and suggestion during my study process. Additionally, I specially thank my friends, my classmates and all other individuals for helps, supports, sharing knowledge and encouraged me throughout the courses in Yangon University of Economics.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AM	-	Assistance Manager
BOD	-	Board of Director
CBM	-	Central Bank of Myanmar
CCPA	-	California Consumer Privacy Act
CEO	-	Chief Executive director
CSR	-	Corporate Social Responsibility
DGM	-	Deputy General Manager
DMD	-	Deputy Managing Director
GDPR	-	General Data Protection Regulation
GM	-	General Manager
GTB	-	Global Treasure Bank
HTTPS	-	Hypertext Transfer Protocol Secure
IT	-	Information Technology
M	-	Manager
MD	-	Managing Director
MLFDB	-	Myanmar Livestock and Fisheries Development Bank
Reg;	-	Regional
SMART	-	Specific, Measurable, Achievable, Relevant, and Time-bound
WU	-	Western Union
YGN	-	Yangon

CHAPTER I
INTRODUCTION

In the digital era, as technology becomes increasingly integrated into daily life, the need for robust cyber security measures becomes more apparent, especially with the rise of cyber threats in sectors like banking. Financial institutions face escalating risks and threats in the evolving digital landscape, underscoring the importance of implementing proactive cyber security strategies. Employees are the most valuable asset for any company, as they significantly influence the organization's success and profitability (Afsana et al., 2016). Recognizing this, the banking sector places significant emphasis on cyber security training practices to equip its employees with the skills and knowledge needed to combat cyber threats. Yozi, N. A. (2018) stated that training and development programs not only assist employees in enhancing their skills and performance but also play an essential role in motivating them.

Employee work performance, coupled with the effective implementation of cybersecurity practices, is an essential for protecting organizational assets and maintaining operational integrity. A well-trained workforce is better equipped to identify and respond to potential threats, improving productivity, efficiency, and finally, organizational success. Thus, examining the effectiveness of cyber security training practices on employee work performance becomes imperative in the context of the banking sector.

Recognizing that cyber security is a collective responsibility, this study focuses on the essential intersection of technology and human behavior. Employee performance is an essential factor in GTB Bank cyber security training, empowering the workforce to recognize and respond to threats effectively.

The bank Global Treasure Bank was established on 15th February 1996 as the Myanmar Livestock and Fisheries Development Bank (MLFDB). It transformed into GTB Bank (Public Company Limited) on 1st July 2013, following approval from the Ministry of National Planning and Economic Development (MNPED), Directorate of Investment & Company Administration (DICA). GTB Bank (Public Company Limited) operates as a commercial bank licensed by the Central Bank of Myanmar (CBM) to engage in various financial activities It holds licenses for domestic banking, money changing, and authorized dealer services, enabling it to offer foreign banking services.

The bank branches must prioritize cyber security due to the digitalization of services.

GTB Bank employees need the knowledge and skills necessary to secure sensitive information and respond effectively to security incidents. By teaching employees little by little each day, the risk of security breaches is reduced, while ownership and accountability among employees are increased. This approach fosters a culture of collective responsibility for cyber security. Bank employees can safeguard sensitive information through cyber security measures, thereby promoting trust in banking services and maintaining the reputation of banking institutions. By reducing financial losses associated with fraud cases, banking organizations can more effectively allocate resources toward innovation, customer service, and strategic initiatives.

The purpose of this study is to determine the effect of cybersecurity training practices on the performance of GTB Bank employees. By examining the impact of cyber security practices on employee performance at GTB bank, the study aims to contribute to developing of more effective cyber security training programs and enhance the overall cyber security resilience within the banking sector.

1.1 Rationale of the Study

In the interconnected digital landscape, the banking sector is confronted with an escalating number of cyber threats and attacks. These threats not only endanger the security of sensitive financial information but also present significant risks to the stability and credibility of financial institutions. Hasan, M. T. (2023) indicated the increasing significance of cyber security, especially in banking, due to the rise of digitization. Most financial institutions are beginning to invest in cyber security measures. It has become essential for GTB Bank to invest in resilient cybersecurity systems.

However, technical solutions alone are insufficient to effectively combat cyber threats. As cyber threats evolve, the skills and awareness of employees tasked with safeguarding an organization's assets must also advance. Employees are the first line of defense against cyberattacks, making their role essential. Since human error is one of the primary causes of security breaches, training is essential to reduce the likelihood of successful cyber-attacks. Enhancing employee’s awareness, knowledge, and skills in identifying and addressing to potential threats is essential for maintaining the security of the organization's digital assets (Von Solms, R., & Van Niekerk, J, 2013).

Cybersecurity training practices are instrumental in equipping employees with the skills and knowledge to navigate the complex landscape of cyber threats. By offering comprehensive training programs, organizations can empower their employees to recognize and mitigate potential risks, thereby enhancing the overall cyber security posture of the organization. Training, particularly in the area of cyber security, is an ongoing process. Practical cyber security training is essential to mitigate risks associated with cyber threats and ensure the integrity and confidentiality of sensitive financial data. As hackers use more sophisticated tactics to exploit systems' vulnerabilities, the need for a well-trained workforce to identify and mitigate these risks is paramount. Cybersecurity training is essential for improving employee performance.

Cybersecurity training helps employees recognize phishing attempts and provides them with the knowledge and skills to secure essential information and respond effectively to security incidents (Kim, 2017; Chen et al., 2020). Such training initiatives play a essential role in strengthening the cyber defenses of banking institutions (Lee, 2021). Additionally, cybersecurity training improves employees' skills and confidence in navigating digital environments. These programs empower employees to make informed decisions and take appropriate measures to protect organizational assets, thereby enhancing their work performance. (Amir Elnaga & Amen Imran, 2013).

By implementing comprehensive training programs that blend theoretical knowledge, hands-on skill development, and simulation-based training, banking institutions can enhance their resilience to cyber threats (Robbins & Judge, 2019). Academic reinforcement through empirical studies and theoretical frameworks provides valuable insights into the effectiveness of various training approaches, empowering organizations to tailor their initiatives to the specific needs and challenges of the banking sector (Aguinis & Kraiger, 2009; Green, 2019). By developing robust cybersecurity training programs, banking organizations can not only meet regulatory requirements but also effectively mitigate emerging threats (White, 2018).

A coordinated effort to deal with fraud through cybersecurity initiatives protects individual institutions and strengthens the overall stability and sustainability of the banking industry Cybersecurity training practices play an essential role in enhancing employee work performance and strengthening banking organizations' resilience against evolving cyber threats.

1.2 Objectives of the Study

The objectives of the study are outlined as follows;

(1) To identify the cyber security training practices provided by Global Treasure Bank.

(2) To analyze the effect of cyber security training practices on employee work performance at Global Treasure Bank.

1.3 Scope and Method of the Study

This study primarily focuses on the cybersecurity factors that need attention as digital technology evolves. Specifically, it explores the impact of cybersecurity training on employee work performance in relation to the cybersecurity techniques taught by GTB Bank. The research employed descriptive and quantitative research methods. GTB Bank had 150 branches in Myanmar. The standard questionnaire is collected at random from 250 IT officers and staff, representing over 30% of the total IT staff of 450. In this study, data are collected from both primary and secondary sources. The data collection process employs a simple random sampling method. Primary data is collected through a questionnaire survey method that included open-ended, closed-ended, and five-point Likert scale questions. Secondary data is collected from the GTB bank website, related websites, articles, and research papers.

1.4 Organization of the Study

This study is organized into five chapters. Chapter I begins with an introduction, rationale of the study, objectives of the study, scope and method of the study, and organization of the study. Chapter II describes the theoretical background of cyber security, improving employee awareness, and employee work performance. Chapter III presents the profile of GTB Bank and the cyber security training practices on employee work performance at GTB Bank. Chapter IV next analyzed the collected data. Finally, Chapter V concludes the study with findings, discussions, recommendations, and needs for further research.

CHAPTER II
THEORETICAL BACKGROUND

This chapter examines the theoretical relationship between cyber security training practices and worker performance at GTB Bank. This chapter is divided into sections discussing the theory and early investigations related to this topic. Concepts such as training and development, theoretical models, training procedures, the concept of employee performance, earlier studies, and the conceptual framework of the study is discussed in this chapter.

2.1 Concept of Training

Training is an essential element for organizational success, particularly in the realm of cyber security within the banking sector. Training involves equipping employees with the necessary knowledge, skills, and competencies to effectively perform their job roles (Elnaga & Imran, 2013). This includes imparting specific information, techniques, and procedures related to cyber security practices, protocols, and tools (Bosworth & Kabay, 2002).

Well-designed training programs provide employees with the necessary skills and knowledge. Training is a systematic process designed to enhance knowledge, skills, and competencies among individuals within an organization to enhance their performance and effectiveness in their roles (Elnaga & Imran, 2013). It plays an essential role in aligning employee capabilities with organizational goals and objectives.

Training initiatives help build a skilled and knowledgeable workforce capable of effectively identifying, preventing, and responding to cybersecurity threats (Dash & Ansari, 2022). In the context of GTB Bank, where protecting of sensitive financial data and customer information is paramount, a robust training and development program in cyber security is essential to mitigate risks and safeguard organizational assets.

Cyber security training plays a pivotal role in safeguarding an organization's digital infrastructure and confidential data. Its primary objective is to empower employees with the skills needed to effectively detect, prevent, and respond to various cyber threats. By enhancing awareness and comprehension of cyber security protocols, these training initiatives mitigate the risks associated with cyberattacks, thereby bolstering organization’s defense against potential breaches.

2.1.1 Types of Training

Examining the goals of training can provide a clearer understanding of its different purposes. Ghuman (2010) and Armstrong (2013) categorize the different types of training, highlighting their distinct focuses and objectives.

Technical training focuses on imparting essential skills and knowledge related to cybersecurity tools and systems, covering areas such as network security, encryption techniques, malware analysis, and penetration testing (Ghuman, 2010; Armstrong, 2013). These skills are crucial for daily tasks and performance. Management training is designed for managers and leaders, equipping them with the problem-solving skills and decision-making skill needed to effectively lead teams and manage cybersecurity incidents (Armstrong, 2013).

Incident response training prepares employees to respond swiftly and effectively to cybersecurity incidents. Through simulated scenarios, employees learn to identify, contain, and mitigate the impact of potential breaches. Compliance training ensures that employees understand and follow to cybersecurity regulations, industry standards, and organizational policies, including data protection laws and regulatory requirements specific to banking (Ghuman, 2010).

Role-based training customizes cybersecurity education to fit the responsibilities of different roles within the organizational roles, enhancing practical skills and problem-solving abilities relevant to specific job functions. Continuous training and skill development are essential for keeping employees updated on evolving cyber threats and trends. This includes attending workshops, webinars, and pursuing certifications to maintain proficiency in cybersecurity practices.

Simulation-based training involves realistic scenarios that simulate cyber threats, allowing employees practice incident response and improve their ability to identify and effectively mitigate security breaches (Armstrong, 2013). By selecting and combining these training methods, banks can ensure that their employees are well-prepared to handle cyber threats, enhancing overall organizational security and performance.

2.1.2 Cyber Security Awareness Training

Cybersecurity awareness training at GTB Bank is the foundational pillar for all employees, aiming to impart fundamental knowledge about cybersecurity risks and best practices. Participants learn basic cyber hygiene practices such as effective password management and safe browsing habits. They are also taught how to identify and mitigate common threats, such as phishing attacks and social engineering techniques. Furthermore, the training emphasizes the secure handling of sensitive information and outlines clear procedures for promptly reporting cybersecurity incidents (Ghuman, 2010; Armstrong, 2013).

The training instructs employees on cybersecurity best practices, policies, and procedures, helping them understand the importance of cybersecurity and instructing them on how to identify and respond to potential security threats such as phishing attacks, social engineering attempts, and suspicious emails. It covers several essential areas to enhance users' understanding and practices. Phishing awareness teaches users to identify phishing emails, malicious links, and fraudulent websites. Password management education focuses on creating strong, unique passwords and using password managers for improved security. Social engineering awareness provides insights into methods used by cybercriminals to manipulate users into revealing sensitive information (Ghuman, 2010).

Data privacy training emphasizes safeguarding personal and sensitive information, complying with regulations like GDPR or CCPA, and implementing strategies to minimize data collection and retention. Safe browsing habits encourage users to verify website authenticity, use secure connections (HTTPS), and exercise caution when downloading files or clicking links. Device security training emphasizes the essential need to keep software and operating systems up to date to safeguard against vulnerabilities (Armstrong, 2013).

After completing the training, employees gain an understanding of various cybersecurity threats, including malware infections, phishing attacks, ransomware, data breaches, insider threats, and denial-of-service (DoS) attacks. They are also familiar with best practices to mitigate these threats, including using strong passwords, updating software regularly, employing firewalls and antivirus software, encrypting data, conducting security audits, providing ongoing cybersecurity awareness training, enforcing least privilege access, and implementing data backups (Ghuman, 2010; Armstrong, 2013).

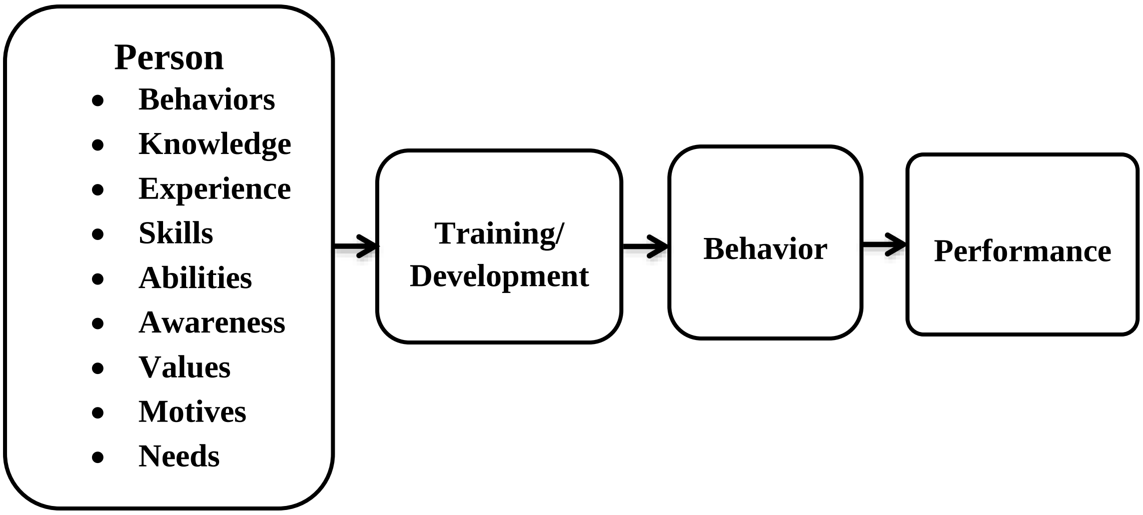
2.2 Related Models

This study employs the Performance Pathway Model and the Kirkpatrick Model of Training Evaluation.

The Performance Pathway Model

Jones, T. E. (2019) presented a Performance Pathway Model that links training and development to enhanced job performance, advocating for their integration into employee engagement strategies to foster a positive work culture.

Figure (2.1) Performance Pathway Model



Source: Jones. T. E. (2019).

The model comprises four components:

This model explains how individuals possess unique qualities when they begin a job. Successful training and development initiatives depend on a thorough understanding of the individual. It emphasizes eight key factors influencing job performance: knowledge, experience, skills, abilities, awareness, values, motives, and needs. These factors evolve as individuals become more familiar with their roles. For high achievers, these changes are typically positive, with improvements in their skills and motivation. They are prepared for change and adapt well to new challenges. Therefore, it is essential to assess the current skills and knowledge of each employee.

Training helps with short-term needs by improving skills quickly. Development emphasizes long-term growth by nurturing each employee's potential and fostering continuous improvement over time. An organization’s philosophy on training and development affects how individual skill levels are maintained. Both aspects significantly boost employee engagement and productivity, fostering a strong workplace culture.

After implementing training and development programs, organizational leaders should monitor employee behavior to measure their acceptance or resistance to the necessary changes for organizational success. Gathering feedback from employees regarding these initiatives is essential. but it must be analyzed within the broader context of the organization’s culture.

Closely observing job-related behaviors enables leaders to determine whether employees are embrace or resist change. Proactive employees tend to embrace new initiatives and drive change, while those who prefer the status quo avoid new tasks and cling to old habits unless closely monitored.

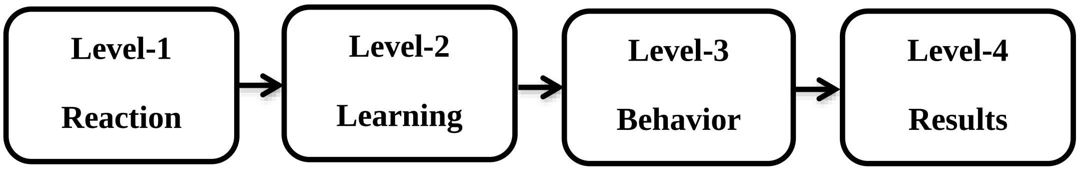
Performance results from how a person interacts with their job demands, training, development, and behaviors. It is the endpoint where leaders can see what is going well and what is not. However, it is also a starting point—a place to begin anew. With this information, leaders can help low performers and underachievers understand where is improve.

The Kirkpatrick model

Cyber security training be designed, implemented, and evaluated to meet the dynamic needs of today workforce. The Kirkpatrick Model is a widely utilized framework for assessing the effectiveness of training programs. Developed by Dr. Donald Kirkpatrick in the late 1950s, the model consists of four levels of evaluation, each designed to measure a different aspect of training impact. The four levels of the Kirkpatrick Model are Reaction, Learning, Behavior, and Results.

Kirkpatrick’s four levels of training evaluation (Kirkpatrick, 2016) are integrated, along with modern evaluations of cyber security training effectiveness. By integrating Kirkpatrick model with modern evaluations of cyber security training effectiveness, organizations can gain a comprehensive understanding of how well their training programs are preparing employees to mitigate cyber risks and contribute to organizational resilience in today digital landscape.

Figure (2.2) The Kirkpatrick Model of Training Evaluation



Source: Kirkpatrick Evaluation Model.

The reaction level focuses on participants' immediate responses to the training, including how well they liked it. By assessing satisfaction and engagement, organizations can identify issues with the training content, delivery, or environment and make necessary improvements. At the Learning level, the focus shifts to measuring the extent to which participants have acquired the intended knowledge, skills, or attitudes from the training, assessing how much they have learned. The Behavior level evaluates the extent to which participants apply what they have learned when they return to their jobs, focusing on changes in behavior and the transfer of knowledge and skills to the workplace, assessing how well they have applied their learning to their work. Finally, the Results level measures the broader impact of the training on organizational performance, assessing outcomes such as increased productivity, improved quality, reduced costs, higher sales, and enhanced employee performance, and evaluating the return on investment from the training. This level seeks to determine whether the training has contributed to achieving the organization's goals and objectives.

Each level of the Kirkpatrick Model builds on the previous one, providing a comprehensive approach to evaluating training effectiveness. By systematically measuring reaction, learning, behavior, and results, organizations can gain valuable insights into the impact of their training programs and make and make informed, data-driven decisions to improve future training initiatives (Kirkpatrick & Kirkpatrick, 2006). The evaluation of training effectiveness involves measuring the progress of employees' knowledge, skills, and behavioral patterns within the organization resulting from the training program.

2.3 Training Effect on Employee Behavior

Employee behavior in the workplace is significantly influenced by training initiatives designed to enhance skills, knowledge, and attitudes toward organizational goals (Smith, 2023). Effective training programs not only impart technical skills but also shape employee attitudes and behaviors, enhancing job performance and supporting organizational objectives (Jones & Brown, 2021). Specifically, in the context of cyber security training, employees' adherence to security protocols, awareness of cyber threats, and responsiveness to security incidents are critical aspects of their behavior influenced by training interventions (Johnson et al., 2020).

In a study examining cyber security training practices in banking sectors, Smith (2023) found that comprehensive training programs led to improved employee behavior regarding compliance with security policies and proactive engagement in cyber defense measures. This positive shift in employee behavior contributes to enhanced organizational security and resilience against cyber threats (Brown & White, 2019).

2.4 Employee Work Performance

Employee work performance is essential as it directly impacts operational integrity, customer satisfaction, and overall organizational success. Understanding and enhancing employee performance is a critical aspect of organizational success. Employee work performance is an essential factor in organizational success, reflecting how effectively and efficiently employees execute their job responsibilities. It encompasses a range of factors, including productivity, quality of work, adherence to deadlines, and the ability to meet or exceed set objectives (Smith, J. 2020).

In the context of Bank, employee work performance is measured not only by traditional metrics such as the volume of tasks completed or customer satisfaction but also by the ability to maintain operational integrity in a highly regulated financial environment (Jones, 2021). This includes the capability to adhere to cyber security protocols, which are essential in protecting the bank’s digital assets and customer information (Adams, R.2022).

Integrating cybersecurity training into employees' professional development is a key factor that influences their performance. Proper training ensures that employees are well-versed in identifying and mitigating cyber threats, thereby minimizing the risk of data breaches and strengthening the bank's overall security framework (White, 2018). Consequently, cyber security training directly impacts employee work performance by equipping staff with the necessary skills and knowledge to perform their duties securely and effectively (Kim, S. 2017).

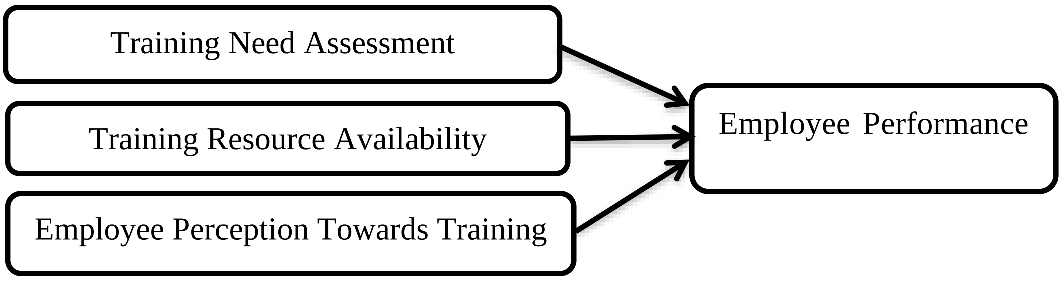
Analyzing the effects of cyber security training on employee work performance at the bank can provide valuable insights into how these training programs enhance the bank's overall efficiency, reliability, and security operations (Lee, H. 2021). Understanding this relationship can help in creating more effective training initiatives that enhance individual performance and strengthen the institution’s resilience against cyber threats. (Green, 2019; Taylor, 2020).

2.5 Previous Studies

This study examined the relationships between training needs assessment, resource availability, perception, and employee performance within the Mekelle City Education Bureau (TREB) in the Tigray Region, Ethiopia. It explores how employee demographics and training assessments influence performance, evaluates the role of training resources management, and examines how employee perceptions of training impact their overall performance. The research provides insights for improving organizational strategies to enhance employee productivity.

This study utilized a descriptive research design with a quantitative approach, employing a cross-sectional method for data collection. It focused on government secondary school teachers and educational institution leaders in Mekelle City, totaling 279 individuals. A multi-stage sampling technique was employed, beginning with district and school selection, followed by simple random sampling of teachers and educational leaders. The conceptual framework is structured as follows:

Figure (2.3) The Effect of Training on Employee Performance


Training Need Assessment
Training Resource Availability
Employee Perception Towards Training
Employee Performance

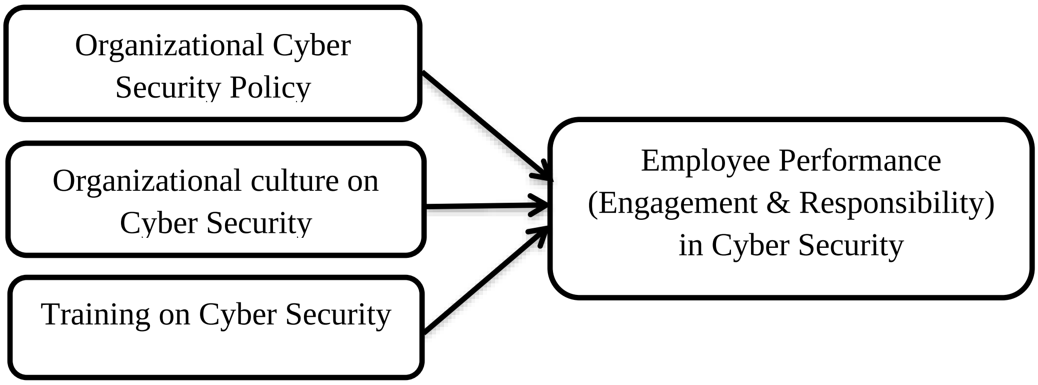
Source: Gebrehiwot, G. D., & Elantheraiyan, P. (2023)

The results suggest that while training needs assessment and resource availability significantly impact employee performance, employee perception of training is not a significant determinant. These recommendations apply not only to the

Tigray Region Education Bureau (TREB) but also to other institutions, with the goal of enhancing training practices worldwide and ultimately improving both employee and organizational performance.

According to Figure (2.4), Md Tareq Hasan's (2023) study focuses on Employee Engagement and Responsibility for a Secure Digital Environment (SDE) in the Selected Branch. This study emphasized the growing importance of cyber security in various sectors, particularly banking, due to increasing digitization. It examines employee engagement and responsibility in cybersecurity at Public Bank Limited, Nandina Branch, using a quantitative research approach and a linear regression model. The study analyzes the relationship between employee engagement and responsibility and factors such as organizational cybersecurity policy ratings, organizational culture, and training quality.

Figure (2.4) Employee Engagement and Responsibility in Cyber Security

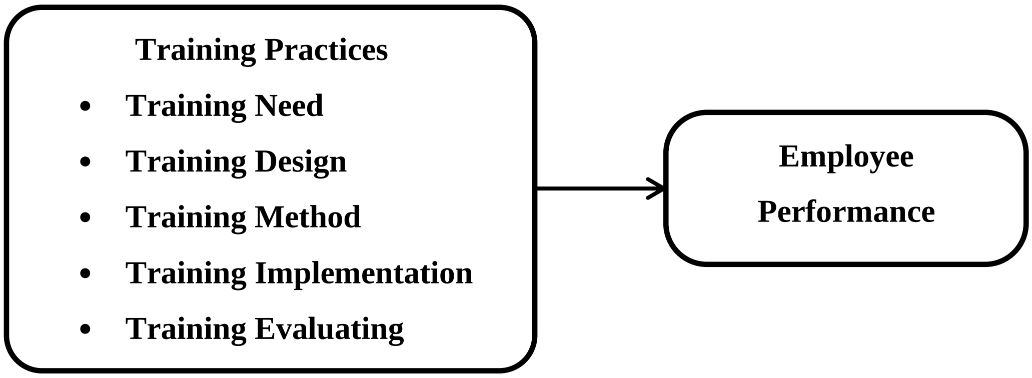

Organizational Cyber Security Policy
Organizational culture on Cyber Security
Training on Cyber Security
Employee Performance (Engagement & Responsibility) in Cyber Security

Source: Md Tareq Hasan (2023)

Data collected through employee surveys offers insights into fostering a cyber security culture and improving digital environments for sustainable business practices. The study also suggests avenues for future research, emphasizing the role of human factors in establishing effective secure digital environments. This study recommends enhancing employee engagement and responsibility by developing robust policies, cultivating a supportive culture, and implementing effective training programs. These measures can improve employees' understanding, awareness, attitude, and skills related to cyber security practices.

According to Figure (2.5), Melaku Habtamu Bekele (2021) examined the effect of training and development on employee performance at Jimma University. The primary objectives of this study are three parts: firstly, to examine the current training and development practices at Jimma University; secondly, to investigate the effect of training and development need assessment, method and design on employee performance; and thirdly, to analyze the effect of the implementation and evaluation of these training and development programs on employee performance. There were two variables Training and Development (Independent) and Employees' performance and productivity (Dependent). This study used a cross-sectional survey, and data was collected from 383 employees at the university, who were chosen using a simple random sampling method. The conceptual framework is structured as follows:

Figure (2.5) The Effect of Training & Development on Employees Performance



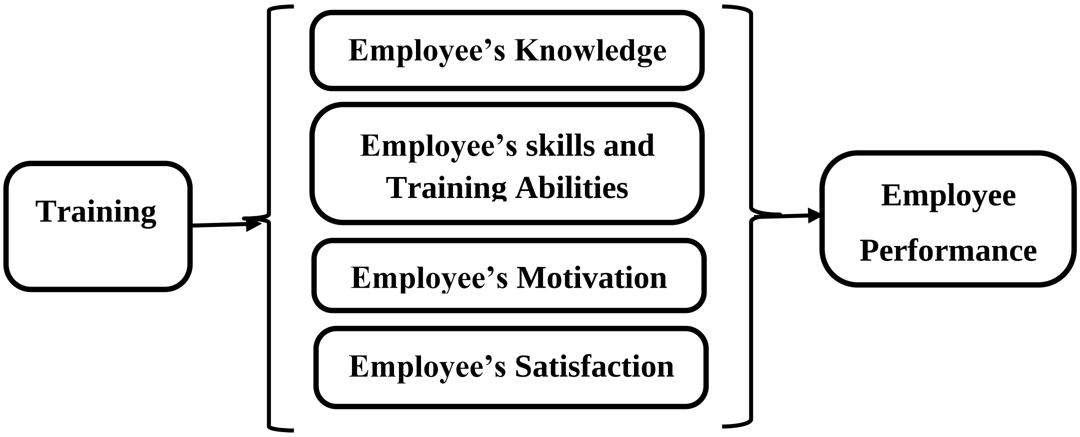
Source: Melaku Habtamu Bekele (2021)

The study revealed a positive, statistically significant correlation between training and development and employee performance. The findings highlighted the importance of practical and systematic training and development practices. The study recommended that top management and training coordinators focus on employee training and development, regularly assess outcomes, and ensure that training programs align with organizational objectives.

According to Figure (2.6), Athar and Shah (2015) conducted a study to observe how training needs are established, the effectiveness of training methods in banks, and their influence on employee performance. The purpose of their research was to identify the factors influencing training in Karachi's banks and how these factors affect employee performance. Their literature review revealed that training is essential for enhancing employees' knowledge, motivation, satisfaction, skills, and abilities.

Training also fosters teamwork and integrity and positively contributes to employee performance development. The conceptual framework is structured as follows:

Figure (2.6) Impact of Training on Employee Performance



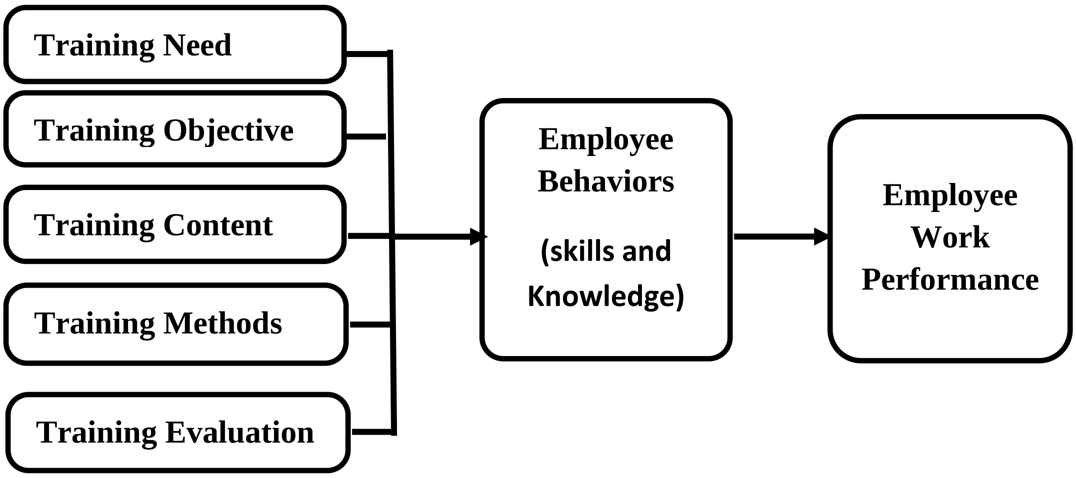
Source: Athar and Shah (2015)

The findings indicated that training positively impacts employee performance in Karachi's banks, as demonstrated by a training framework designed to achieve organizational strategic goals.

2.6 Conceptual Framework of the Study

The conceptual framework of this study is developed based on the previous studies conducted by Melaku Habtamu Bekele (2021) on examining the effect of training and development on employee performance at Jimma University. By Athar and Shah (2015) examined the effect of training and development on employee performance at Jimma University. The success of the cybersecurity training program for employees can be assessed using the Kirkpatrick model, as described in theoretical principles and earlier research. The study considered independent variables such as cybersecurity training needs, training objectives, training context, training methods, and training evaluation based on previous studies. The conceptual framework of this study integrates key elements relevant to cybersecurity training practices and employee work performance at GTB Bank. The conceptual framework is structured as follows:

Figure (2.7) Conceptual Framework of the Study



Source: Own compilation (2024)

According to the conceptual framework, the results are provided to gather empirical data to assess employee performance regarding the efficacy of cybersecurity training procedures at GTB Bank. This study highlights the imperative for financial institutions to invest in comprehensive and continuous training programs that address the unique challenges of the cybersecurity landscape. The findings indicate that expanding and deepening cybersecurity training can significantly enhance employee work performance, improve IT knowledge, instill best practices, and strengthen overall security posture. This approach offers a competitive advantage in the increasingly digital financial environment.

CHAPTER III
ORGANIZATION BACKGROUND AND CYBER SECURITY TRAINING PRACTICES OF GTB BANK

This chapter presents the profile of Global Treasure Bank's excellence built over 27 years of operation. It describes the foundation of the bank, organizational structure, vision, mission, objectives, core values, motto, financial services, and Training and Development programs.

3.1 Profile of GTB Bank

GTB Bank was established on February 15th, 1996, as the Myanmar Livestock and Fisheries Development Bank under License Number MaBaBa/P-15 (2) 96, in accordance with the laws governing Financial Institutions of the Central Bank of Myanmar. It transitioned into Global Treasure Bank (Public Company Limited) on July 1st, 2013, following approval from the Ministry of National Planning and Economic Development (MNPED), Directorate of Investment & Company Administration (DICA), as per its letter No. Yaka-8 (Ga Nga) 001/2013 (010995) dated August 27, 2013. Founded as a public company limited by shares, GTB Bank operates as a commercial bank authorized by the CBM to undertake various financial activities. It possesses licenses for domestic banking, money changing, commercial bank services, and authorized dealer services, enabling it to provide foreign banking services. As the bank's service experience grows, its development accelerates and progresses in parallel with other private banks.

To enhance its employee working capacity, the bank conducts training courses in financial services and cyber security, and staff also participate in competency training and workshops organized by the CBM. In order to provide excellent banking services and ensure customer satisfaction and convenience, GTB Bank has expanded its domestic banking network to include (39) branches in Yangon Division, (16) branches each in Mon, Ayeyarwady, and Rakhine Divisions, (15) branches in Bago Division, (14) branches each in Mandalay and Saging Divisions, (13) branches in Magway Division, (12) branches in Tanintharyi Division, (7) branches each in Naypyitaw and Shan State, (6) branches in Kayin State, and (1) branch in Kayah State. As one of the leading banks in Myanmar, GTB Bank provides banking services through 176 branches across the country. GTB bank has opened 176 branches across Myanmar, and currently provides business services from 150 branches.

GTB bank has clearly defined corporate objectives, which the organization must execute and understand to achieve its mission, vision, and corporate values. The vision of GTB Bank is to become one of the foremost banking service providers in Myanmar, fostering long-term growth by delivering superior services and enhanced financial products. As a leading bank in Myanmar, GTB bank is committed to delivering efficient banking services and building trustworthy, reliable, and successful relationships with all stakeholders. GTB Bank is committed to creating value for our customers.

The primary aim of GTB Bank is to offer robust financial support to entrepreneurs, fostering the growth of various business sectors committed to delivering efficient banking services and Additionally, the bank strives to enhance its commercial functions efficiently. The motto of GTB bank, "Your Dream, Your Success, Global Treasure Bank," reflects its commitment to these objectives. The standards and principles guiding our behavior and interactions with customers and staff are: Customer Focus: Customer First, Integrity: Do what is right, Respect: Value everyone, Teamwork and Operational Excellence: Provide the best services as a team, Innovation: Embrace technology and be creative.

In the 2017-2018 financial year, GTB Bank enthusiastically participated in philanthropic activities under the " Global Treasure Heart Social Support Association." GTB bank donated to CSR programs, supporting the well-being of communities in healthcare, natural disaster rehabilitation, and community development, such as rural power supply and water supply. GTB also aids schools for disabled children, nutrition programs for hospitalized people, homes for the aged, and cancer foundations.

GTB has been offering foreign banking services under the Authorized Dealer License issued by the Central Bank of Myanmar. In this capacity, GTB bank has established Nostro Accounts with 10 Correspondent Banks, enabling it to provide a range of foreign banking services, including Export & Import Services, Bank Guarantee Services, and Trade Financing Services. Furthermore, GTB bank is affiliated with Western Union, facilitating international transfers to and from over 200 countries. Myanmar citizens working abroad can send remittances, which can be withdrawn at any GTB branch, including the Head Office, within minutes.

These relationships fulfill customers' needs in international banking and trade finance services. GTB bank is committed to developing and maintaining long-term partnerships with other financial institutions to grow trade finance transactions, money transfer services, and international banking services.

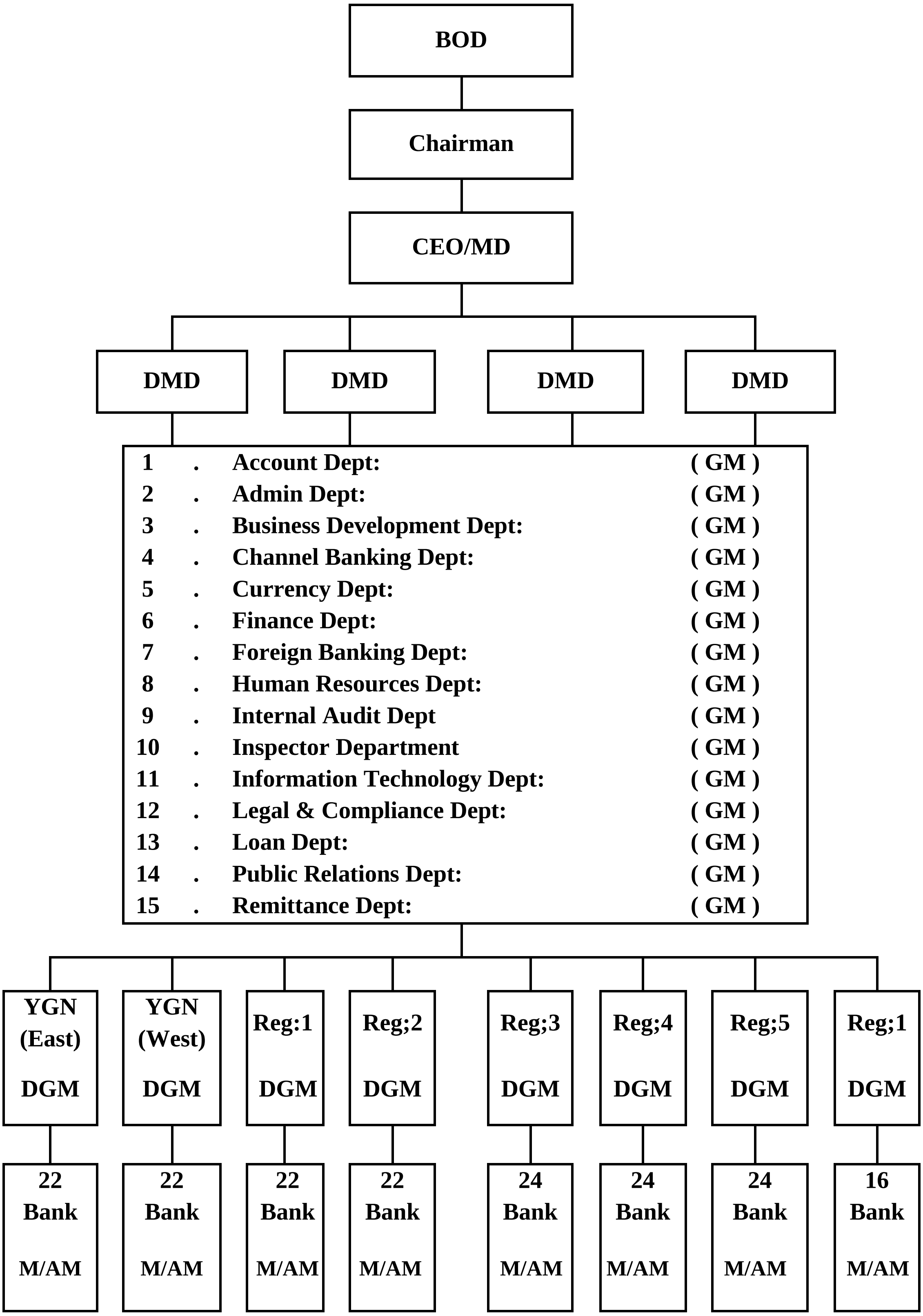
GTB Bank prioritizes continuous professional development for its employees by offering comprehensive training programs designed to enhance their skills and competencies. These programs cover various aspects of banking operations, customer service, financial management, and the latest technological advancements. This ensures that the staff is equipped to meet the evolving needs of the bank and its customers.

3.2 The Organization Structure of GTB Bank

GTB bank is managed by the Board of Directors (BOD) elected by the shareholders, consisting of 14 members. One member is elected as the Chairman of the Board. Additionally, two Independent Non-Executive Directors are appointed at the Annual General Assembly Meeting to provide impartial advice, independent of management. BOD Meetings are convening at least once a month to address essential matters stipulated in laws and the Articles of Association, as well as to make essential decisions related to management policy and strategy.

The Managing Director serves as the Chief Executive Officer of the bank and oversees the senior management. As of the 2023-2024 financial year, GTB bank employs over 3,000 staff members. The GTB Bank’s head office consists of 15 departments. Through these 15 departments, eight regions are divided and the branches in GTB bank are closely supervised. The organizational structure of the bank is as follows:

Figure (3.1) The Organization Structure of GTB


BOD
Chairman
CEO/MD
DMD
DMD
DMD
DMD
1 . Account Dept: (GM)
2 . Admin Dept: (GM)
3 . Business Development Dept: (GM)
4 . Channel Banking Dept: (GM)
5 . Currency Dept: (GM)
6 . Finance Dept: (GM)
7 . Foreign Banking Dept: (GM)
8 . Human Resources Dept: (GM)
9 . Internal Audit Dept (GM)
10 . Inspector Department (GM)
11 . Information Technology Dept: (GM)
12 . Legal & Compliance Dept: (GM)
13 . Loan Dept: (GM)
14 . Public Relations Dept: (GM)
15 . Remittance Dept: (GM)
YGN (East) DGM
YGN (West) DGM
Reg:1 DGM
Reg;2 DGM
Reg;3 DGM
Reg;4 DGM
Reg;5 DGM
Reg;1 DGM
22 Bank M/AM
22 Bank M/AM
22 Bank M/AM
22 Bank M/AM
24 Bank M/AM
24 Bank M/AM
24 Bank M/AM
16 Bank M/AM

Source: GTB Bank (2024)

3.3 GTB Bank Product and Services

GTB Bank provides a full range of retail and corporate banking facilities for its customers. These include Deposits, Loans, Domestic and International Remittances, Core Banking System, Card Business System, Internet Banking/Mobile Banking, Foreign Exchange, Trade Finance, and GTB Pay. There are many types of deposit accounts at GTB Bank, including Savings Deposits, Current Deposits, Fixed Deposits, Call Deposits, Minor Savings Deposits, various types of Special Deposits, Certified Cheques, Payment Orders, and Performance Guarantees. For Loan Services, the types of loans and collateral offered are Demand Loans, Government Staff Loans, and Hire Purchase.

GTB Bank is not just a branch of GTB, but to branches of other banks Money can be transferred through CBM net system. For international remittances, customers can quickly receive funds at the nearest GTB branch using "Western Union," which provides remittance services to over 200 foreign countries. Foreign exchange is one of the functions of GTB’s foreign banking system. Customers can exchange three foreign currencies: the US Dollar, Euro, and Singapore Dollar.

3.4 Training Course Provided by GTB Bank

GTB bank recognizes the essential importance of cyber security in the contemporary digital landscape and has developed a rigorous training program to empower employees with essential knowledge and skills. The Bank offers three main cyber security training courses, in addition to other types of training courses. This program encompasses Cyber Security Awareness Training, Advanced Cyber Security Training, and Linux for Cyber Security Training. Table 3.1 displays these courses.

The Cyber Security Awareness Training, conducted over one to three days, focuses on fundamental cyber security concepts, including recognizing and mitigating phishing attacks, enhancing awareness and resilience, and ensuring all personnel receive timely instructional sessions. The training is facilitated by IT professionals through online sessions via Zoom Meetings, with provisions made for employees who miss sessions to attend subsequent training sessions.

The Advanced Cyber Security Training aims to deepen employees' understanding of cyber security techniques and tools, equipping technical teams to safeguard digital infrastructure of the bank against evolving threats. This training encompasses Instructor-Led Training (ILT), Online Training, and On-the-Job Training programs. The program covers network security protocols, firewall configurations, intrusion detection and prevention systems (IDS/IPS), proactive threat-hunting strategies, and vulnerability management. This comprehensive training ensures that participants can systematically identify, assess, and address security weaknesses, maintaining robust and up-to-date network defenses.

The Linux for Cyber Security Training is an On-the-Job Training initiative where participants gain practical experience by working on real projects. Led by hired instructors and experienced cyber security professionals from the bank, this course covers essential topics such as Linux fundamentals (e.g., operating system introduction, primary command-line usage, and file system management), security concepts (e.g., user and group management, firewall configuration, and system hardening), and the deployment and utilization of essential cyber security tools (e.g., Wireshark, Metasploit, Nmap). Participants also learn about Linux's role in server environments, managing web and database servers, implementing security measures, and conducting hacking and penetration testing using Kali Linux. The course emphasizes best practices, including system updates, strong authentication methods, and regular security audits.

Table (3.1) Cyber Security Training Course Provided by GTB Bank

Sr	Level of Employee	Training Types	Objective	Main Subject of training	Trainer	Training Period
1	All employees at GTB Bank.	Information Security Awareness Training (Online Training-Zoom Meeting)	Impart fundamental knowledge (about cybersecurity risks and best practices)	Cybersecurity Threat Landscape •Understanding and protecting everyday cyber threats • Passwords • Phishing • Malware • System Security • Incident Reporting • Strategy & Tactic	Internal	1 to 3 days (Part-Time)
2	IT staff	Advanced Cybersecurity Training (Instructor-Led Training (ILT), Online Training and On-the-Job Training)	• Deepen understanding of cybersecurity techniques and tools • Equip technical teams to safeguard the bank's digital infrastructure against evolving cyber threats	Network security protocols • Firewall configurations • Implementation of intrusion detection/prevention systems (IDS/IPS) • Proactive threat-hunting strategies • Vulnerability management	External + Internal	Ongoing
3	IT staff	Linux for cyber security training (On-the-Job Training)	employees with the knowledge and skills to secure Linux systems, identify and mitigate security threats, and effectively use Linux-based cybersecurity tools.	Linux Fundamentals • Security Concepts • Cybersecurity Tools • Server Usage • Hacking and Penetration Testing • Incident Response • Best Practices	External + Internal	Ongoing

Source: GTB Bank Survey Data (2024)

GTB Bank comprehensive training courses underscore its commitment to maintaining a high standard of cyber security across all facets of its operations. By equipping employees with specialized knowledge and skills tailored to their roles, GTB Bank not only fortifies its defenses against cyber threats but also fosters a culture of vigilance, compliance, and continuous improvement in cyber security practices. This proactive approach ensures that GTB Bank remains resilient in safeguarding sensitive data, protecting customer trust, and upholding its reputation as a secure financial institution in the digital age.

3.5 Features of the Cyber Security in Myanmar

The advent of the internet and information technology has dramatically transformed the cyber security landscape in Myanmar. Financial institutions and corporations are working to integrate advanced cybersecurity measures to safeguard a broader range of services and an expanding client base, both locally and globally. For example, GTB Bank has utilized these technologies to strengthen its cyber security infrastructure, reduce vulnerabilities, and secure transactions across its 150 branches.

To keep pace with the rapidly changing cybersecurity landscape, GTB Bank continuously modernizes its operations and IT infrastructure. The implementation of advanced cybersecurity technologies is essential for modern banking operations. This project not only enhances operational efficiency of the bank but also strengthens its defenses against cyber threats.

The future of cyber security in Myanmar involves every division within financial institutions, benefiting banks, customers, and employees alike. Enhanced cyber security measures ensure the protection of customer data, secure financial transactions, and provide a safe digital banking environment. By adopting comprehensive and modern cyber security frameworks, financial institutions in Myanmar can build trust and confidence among their clients while safeguarding their operations against cyber threats.

3.6 Cyber Security Training Practices at GTB Bank

GTB Bank emphasizes robust cyber security training to equip employees with essential skills and knowledge. GTB bank provides cybersecurity training with both internal and external instructors through on-the-job training and Zoom sessions are integrated with employees' actual responsibilities. These training programs focus on identifying and mitigating cyber threats, adhering to best security practices, and leveraging advanced tools and technologies. By prioritizing continuous learning and skill development, GTB Bank ensures its staff remains vigilant and capable of safeguarding customer data and maintaining the integrity of banking operations.

3.6.1 Training Needs

Training needs assessment at GTB Bank involves identifying the specific cyber security skills and knowledge gaps among employees. This process ensures that the training programs are tailored to address the actual needs of the workforce, enhancing their ability to protect the digital infrastructure of the bank. By evaluating current cyber security practices, incident reports, and employee feedback, GTB Bank determines the most essential areas requiring improvement and tailors its training programs accordingly. This systematic approach ensures the training is relevant, effective, and aligned with the GTB Bank's strategic goals.

3.6.2 Objective of Cyber Security Training

The primary objective of cyber security training at GTB Bank is to equip employees with the necessary knowledge and skills to protect the digital assets of the bank, ensure compliance with regulatory requirements, and cultivate a culture of cybersecurity awareness. The cyber security training has successfully achieved the following goals:

1. Enhancing employes ability to recognize and thwart phishing attempts.
2. Heightening awareness and resilience against various cyber threats.
3. Mitigating risks associated with cyberattacks.
4. Ensuring all personnel understand and adhere to cyber security best practices.
5. Empowering IT staff with advanced skills to manage and secure the IT infrastructure of GTB Bank.
6. For different levels of bank staff, the responsibility for organizing and distributing training activities, including various in-service training, on-the-job training, and off-the-job training.

3.6.3 Content of Cyber Security Training

The cyber security awareness training program at GTB Bank includes theoretical and practical elements to enable the transfer of new knowledge and skills.

The creation of a training program at GTB Bank follows a structured process. First, the Training and training department identifies the training requirements. Subsequently, they plan the demonstration and training program, detailing a list of training modules, proposed dates and times, the name of the trainer, the duration of each training session, the training objectives, and an outline for each module. The training and testing of the planned function are essential phases in the cyber security training project, as these are the stages where many projects face challenges. The content of GTB Bank cyber security training is thorough and encompasses a broad array of topics to address the diverse needs of employees.

At GTB Bank, all employees participate in a comprehensive Information Security Awareness Training program delivered through online Zoom meetings. The objective of this training initiative is to equip employees with fundamental knowledge essential for cybersecurity, emphasizing the recognition and mitigation of cyber threats. Key topics covered include understanding the evolving cyber threat landscape, safeguarding against common risks such as phishing and malware, implementing robust password security practices, ensuring system integrity, and adhering to incident reporting protocols. Conducted over a flexible period of 1 to 3 days by internal trainers, the program aims to enhance employees' resilience against cyber threats and strengthen the bank's overall cybersecurity posture.

The advanced cyber-security training program for IT staff aims to deepen their understanding of cybersecurity techniques and tools while equipping technical teams to safeguard the bank's digital infrastructure against evolving threats. This comprehensive three-month training, led by both external and internal trainers, will focus on the implementation of intrusion detection systems and prevention systems (IDS/IPS), proactive threat-hunting strategies, and vulnerability management. The training will be delivered through instructor-led sessions, online modules, and on-the-job training, ensuring a thorough and practical learning experience. The program is designed to enhance the network security protocols, firewall configurations, and the ability to manage and mitigate cyber risks effectively.

The Linux for Cyber Security training program for IT staff aims to equip employees with the knowledge and skills to secure Linux systems, identify and mitigate security threats, and effectively use Linux-based cyber security tools. This ongoing training, conducted by both external and internal trainers, covers Linux fundamentals, security concepts, deployment and usage of cyber security tools, server management, hacking and penetration testing, incident response, and best practices. The training is delivered through on-the-job methods, ensuring that participants gain practical, hands-on experience in securing Linux environments and responding to various cybersecurity challenges.

3.6.4 Cyber Security Training Methods

The Cyber Security Training Course employs diverse methodologies to accommodate various learning styles, ensuring thorough coverage and effective knowledge transfer. Interactive workshops provide hands-on sessions that allow participants to apply cybersecurity principles practically. Simulations and drills, including phishing simulations and incident response exercises, enhance real-world readiness. Certificate programs are available to validate cybersecurity expertise and encourage continuous learning. Instructor-led training sessions are facilitated by IT professionals and cyber security experts, while online training sessions conducted via Zoom Meetings ensure remote accessibility. Additionally, hands-on training workshops provide practical experience, and on-the-job training offers real-world experience through project work under the guidance of experienced professionals.

3.6.5 Evaluation of Cyber Security Training

The evaluation of cyber security training programs at GTB Bank is essential for assessing the effectiveness of the training sessions. This evaluation process involves various methods to understand the impact of the training on employees' skills and knowledge, identify areas for improvement, and ensure continuous enhancement of the training programs. Various methods are employed to evaluate the impact and effectiveness of cybersecurity training programs comprehensively.

Firstly, knowledge assessments are conducted both before and after training sessions to quantify the increase in understanding of cybersecurity concepts covered during the training. Secondly, skills testing is implemented to evaluate participants' practical application of cybersecurity skills acquired through simulations or practical tests. Additionally, behavioral changes are monitored to gauge shifts in employee practices concerning cybersecurity protocols, such as adherence to security measures and prompt reporting of suspicious activities. Feedback surveys are essential for gathering participant perspectives on the relevance, clarity, and effectiveness of the training content and delivery. Performance metrics, including key indicators related to cybersecurity incidents, employee compliance with security policies, and overall security posture, are tracked to measure the training's impact on organizational security resilience. Follow-up sessions are also conducted to reinforce learning and address any identified gaps post-training. Incident reports provide insights into the frequency and severity of cybersecurity incidents or breaches before and after training, helping assess the training's effectiveness in reducing security risks.

Lastly, compliance rates with cybersecurity policies and best practices among trained employees compared to their non-trained counterparts are analyzed to determine the program's effectiveness in promoting consistent security practices across the organization. By continuously assessing and refining its cyber security training practices, GTB Bank ensures its employees well-prepared to handle the evolving challenges of the digital landscape, thereby maintaining a robust cyber security posture.

3.6.6 Employee Behavior

Employee behavior at GTB Bank encompasses the actions, attitudes, skills, knowledge, and interactions exhibited by staff members in the workplace. It includes adherence to organizational policies and procedures, professionalism in customer interactions, teamwork and collaboration with colleagues, and proactive engagement in maintaining cybersecurity protocols. At GTB Bank, desired employee behaviors also involve a commitment to continuous learning and improvement, particularly in cybersecurity practices. This includes vigilance in identifying potential security threats, adherence to established security protocols, and effective communication within teams to mitigate risks promptly. Employee behavior plays a critical role in shaping the bank's overall operational efficiency, customer satisfaction levels, and ability to maintain a secure digital environment amidst evolving cyber threats.

3.6.7 Employee Work Performance

The effect of cyber security training on employee work performance is a vital aspect of GTB Bank’s overall training strategy. Employees who undergo thorough cyber security training demonstrate improved performance across several key areas. Employees develop a deep understanding of cyber security concepts and become proficient in using various cyber security tools and techniques, enabling them to address security issues effectively. With improved skills, employees can perform their tasks more efficiently, reducing the likelihood of security breaches and ensuring smoother operations within the organization. Well-trained employees are better prepared to identify and mitigate potential threats proactively, thereby strengthening the overall security of the bank's digital infrastructure. By adhering to established security protocols and best practices, employees ensure regulatory compliance and minimize vulnerabilities across the organization. Additionally, enhanced cyber security knowledge fosters better collaboration among team members, leading to more cohesive and coordinated efforts in maintaining the bank's security.

GTB Bank’s comprehensive training courses underscore its commitment to maintaining a high standard of cybersecurity across all facets of its operations. By equipping employees with specialized knowledge and skills tailored to their roles, GTB bank not only fortifies its defenses against cyber threats but also fosters a culture of vigilance, compliance, and continuous improvement in cyber security practices. This proactive approach ensures that GTB Bank remains resilient in safeguarding sensitive data, protecting customer trust, and upholding its reputation as a secure financial institution in the digital age. In summary, the comprehensive cyber security training at GTB Bank significantly boosts employee work performance, ensuring that the bank remains resilient against cyber threats and operates securely in the digital landscape.

CHAPTER IV
ANALYSIS ON THE EFFECT OF CYBER SECURITY TRAINING PRACTICES ON EMPLOYEE WORK PERFORMANCE AT GTB BANK

This chapter presents the analysis of the effect of Cyber Security Training Practices on Employee Work Performance of GTB Bank. This chapter is organized into two major sections. Firstly, the measurement of the descriptive statistics of the variables. Lastly, the measurements of training practices on employee work performance, as well as an analysis on employee performance level.

4.1 Research Design

This study looked into the cyber security training practices used by GTB Bank in Myanmar. It examines how GTB Bank employees perform in relation to these cyber security training practices. GTB Bank has 150 branches in Myanmar, with about 450 IT officers and staff. A random sample of 150 employees, including IT officers and staff, was chosen, representing over 30% of the workforce. The population size is known, it is calculated based on the Taro Yamane Formula (1967) n=$\frac{N}{(1+Ne^{2})}$, Margin of error (MoE), e = 0.04 based on the research condition. The sample was selected through a simple random sampling method. A questionnaire survey with a structured questionnaire was used to gather the data.

The survey analysis is displayed below using Likert scale ratings of 1 for strongly disagree, 2 for disagree, 3 for neutral, 4 for agree, and 5 for strongly agree. The mean value for the responses was computed using descriptive statistics. The SPSS 25 program was used to analyze the data. The association between the independent variables and the dependent variable was conducted using multiple regression analysis with the entry method.

4.2 Demographic Analysis

This study, to assess the impact of cyber security training practices on employees, a survey involving 150 of GTB Bank's IT employees was conducted. This section provides information about their demographic profile, including age, gender, education level, and employment history (in years). Each characteristic has been analyzed in terms of absolute value and percentage. Table (4.1) presents the analysis results of the respondents' demographic profiles.

Table (4.1) Demographic Profile of Respondents

Sr. No	Description		Number of Respondents	Percentage (%)
1	Gender	Male	53	35%
		Female	97	65%
		Total	**150**	**100%**
2	Age (Years)	18-25	23	15%
		26-35	62	41%
		36-45	49	33%
		46-55	16	11%
		Total	**150**	**100%**
3	Education	Under Graduate	31	21%
		Graduate	106	71%
		Master Degree	13	9%
		Total	**150**	**100%**
4	Job Position	Junior /Senior Assistant	57	38%
		Supervisor /Assist Supervisor	42	28%
		Manager / Assist Manager	45	30%
		Other	6	4%
		Total	**150**	**100%**
5	Years of Experience	Less than one year	26	17%
		1-3 years	27	18%
		4-6 years	35	23%
		7-10 years	27	18%
		More than ten years	35	23%
		Total	**150**	**100%**

Source: Survey Results (2024)

As shown in Table (4.1), The demographic data collected from 150 employees at GTB Bank reveals. Regarding gender distribution, a significant majority of respondents are female, comprising 65% (97 individuals), while males represent 35% (53 individuals). The data indicates that female employees outnumber male employees by almost 2:1, Female respondents are therefore more dominant than male respondents.

In terms of percentages, the age distribution of respondents is as follows: 18-25 years account for 15%, 26-35 years account for 41%, 36-45 years account for 33%, and 46-55 years account for 11%. The data shows a concentration in the 26-35 and 36-45 age groups. The majority of respondents (74%) are between the ages of 26 and 45, which is typically considered the prime working age. The most employees are likely to be experienced and potentially more receptive to advanced cyber security training programs.

The respondents' educational backgrounds are categorized into three groups: undergraduate, graduate, and master's degree. According to the results, 71% of respondents have graduate degrees, 21% have undergraduate degrees, and only 9% have master's degrees. The education levels of the respondents show a high percentage of graduates. With 71% of respondents holding a graduate degree, it is evident that the workforce is well-educated. This high level of education could contribute to better understanding and implementation of cyber security training practices.

The job positions held by respondents are diverse at GTB Bank, with the largest group being Junior/Senior Assistants. Out of the 150 people surveyed, 64 (43%) worked as Junior or Senior Assistants, 42 (28%) as Supervisors or Assistant Supervisors, 38 (25%) as Managers or Assistant Managers, and 6 (4%) in other positions. The respondents' years of working experience are evenly distributed across several categories. Experience levels are quite balanced, with significant portions of the workforce having 4-6 years and more than ten years of experience (23% each). This balance reflects a mix of relatively new and highly experienced employees, which could impact how training programs are received and implemented.

4.3 Reliability Analysis

Reliability analysis is an essential statistical technique to assess the consistency and dependability of measurement instruments or scales employed in research. In the context of this thesis, reliability analysis was conducted to ensure the reliability of the survey instrument used to collect data from employees at GTB Bank regarding cybersecurity training practices and their impact on employee work performance. Five-point Likert scale surveys were employed in the study. The analysis involved evaluating the internal consistency of the survey items, typically measured using Cronbach's alpha coefficient.

Table (4.2) Rules of Thumb for Alpha Result

Cronbach's Alpha	**Strength of Association**
Below 0.6	poor
0.6 to 0.7	moderate
0.7 to 0.8	good
0.8 to 0.9	Very good
Above 0.9	Excellent

Source: Hair Jr., Babin, Money, & Samouel (2003)

Cronbach's Alpha ranges from 0 to 1. A high alpha value may suggest redundant questions, while a low value could indicate insufficient test questions. It is essential to assess the validity of surveys related to employee performance and cybersecurity training practices. Therefore, the study calculated the Cronbach's Alpha test accordingly.

Table (4.3) Cronbach's Alpha Reliability Test

Sr. No.	**Variables**	**No. of Item**	**Cronbach's Alpha**
1	Cyber Security Training Needs	5	0.850
2	Cyber Security Training Objective	5	0.844
3	Cyber Security Training Content	5	0.856
4	Cyber Security Training Method	5	0.910
5	Cyber Security Training Evaluation	5	0.922
6	Employee Behavior	5	0.847
7	Employee Work Performance	5	0.860

Source: Survey Results (2024)

4.4 Descriptive Statistics for Cyber Security Training Practices of GTB Bank

The training needs, the training objectives, the training content, the training method, the performance and behaviors of the trainer, and the training evaluation made up the conceptual model of the study. The findings in this section aim to quantify the impact of each variable on employee output at GTB Bank. The goal of this study was to determine the cyber security training practices offered by GTB Bank and to examine how those practices affected the performance of GTB Bank personnel.

The questionnaire consists of three sections aimed at collecting quantitative data. The first section uses closed-ended structured questions to gather quantitative data, primarily focusing on exploring the demographic profiles of the respondents. Each factor included corresponding statements, which were assessed using a five-point Likert scale ranging from 1 to 5 (with options ranging from 'strongly disagree' to 'strongly agree'). According to Best (1977), the mean values of items on a five-point Likert scale are interpreted as follows:

Table (4.4) Mean Score Interpretation

Total Mean Score	Level
1.00 and 1.80	Strongly disagree
1.81 and 2.60	Disagree
2.61 and 3.40	Neutral
3.41 and 4.20	Agree
4.21 and 5.00	Strongly agree

Source: Best (1977)

This design fits a study of this nature since the researchers looked at the effects of independent variables (cyber security training practices) on the dependent variables (employee behavior and employee work performance).

4.4.1 Cyber Security Training Needs

The study assessed employees' perceptions of the cyber security training needs at GTB Bank through five statements: the necessity of training programs to enhance employee ability, the importance of cyber security training to protect the bank's digital infrastructure, identifying cyber security skills and knowledge gaps, modifying training programs to meet actual needs, and the requirement for employees to complete cyber security training. Each statement was rated on a Likert scale from 1 to 5. The detailed mean values and standard deviations for these statements are presented in Table (4.5) below.

Table (4.5) Cyber Security Training Needs of GTB Bank

Sr. No.	Description	Mean	Std. Dev
1	Training programs are necessary to enhance employee ability.	3.77	0.893
2	Cybersecurity training is essential needed to protect the digital infrastructure of the bank.	3.87	0.857
3	Training needs involve identifying cybersecurity skills and knowledge gaps among employees.	3.83	0.789
4	It is necessary that training programs be modified to meet the actual needs.	3.87	0.816
5	GTB Bank employees are required to complete cybersecurity training.	3.77	0.814
Overall Mean Scores		**3.82**	

Source: Survey Results (2024)

According to Table 4.5, respondents on the training needs for the cyber security training course in GTB bank, particularly emphasizing that Cyber security training is essential to protect the digital infrastructure of the bank and it is necessary that training programs be modified to meet the actual needs, both of which had a mean score of 3.87. Conversely, respondents barely agreed that Training programs are necessary to enhance employee ability and GTB Bank employees are required to complete cyber security training, with a minimum mean score of 3.77. The overall mean score for the training needs was 3.82, indicating that, on average, respondents agree with the importance and necessity of the cyber security training needs at GTB Bank.

4.4.2 Cyber Security Training Objectives

The study assessed employees' perceptions of cyber security training objectives at GTB Bank through five statements. The cyber security training objectives were: clearly defined, aimed at understanding security issues and promoting responsible actions; helped employees understand the importance of cyber security; aligned well with employee work competency; and well-trained employees feel more confident in their ability to identify and address cybersecurity threats, thereby reducing the likelihood of successful attacks. Each statement was rated on a Likert scale from 1 to 5. The detailed mean values and standard deviations for these statements are presented in Table (4.6) below.

Table (4.6) Cyber Security Training Objectives of GTB Bank

Sr. No.	Description	Mean	Std. Dev
1	The cybersecurity training objectives were clearly defined.	3.73	0.851
2	The objectives of cybersecurity training are to understand security issues and to act responsibly.	3.94	0.943
3	The cybersecurity training objectives helped understand the importance of cybersecurity.	3.77	0.998
4	The cybersecurity training objectives at GTB Bank aligned well with employee work competency.	3.83	0.944
5	The cybersecurity objectives are to identify and effectively mitigate potential cyber threats.	3.81	0.960
Overall Mean Scores		**3.82**	

Source: Survey Results (2024)

According to Table (4.6), respondents on the training objective for the cyber security training course in GTB bank, particularly emphasizing that "The objectives of cyber security training are to understand security issues and to act responsibly," which had a mean score of 3.94. Conversely, respondents barely agreed that "The cyber security training objectives were clearly defined," with a minimum mean score of 3.73. The overall mean score for the training objectives was 3.82, indicating that, on average, respondents agree with the cyber security training objectives at GTB Bank. This suggests that the training objectives are perceived as clearly defined, relevant to employees' roles, and effective in enhancing their cyber security awareness and skills.

4.4.3 Cyber Security Training Content

The study evaluated employee perceptions of the cyber security training content at GTB Bank using five statements: The training content provides a platform for technical skills, covers all necessary aspects of cyber security, is easy to understand, the examples and case studies used were relevant to the job, and the training programs provide opportunities to update existing skills and acquire new technologies for employees in cyber security training. Each statement was rated on a Likert scale from 1 to 5. The detailed mean values and standard deviations for these statements are presented in Table (4.7) below.

Table (4.7) Cyber Security Training Content of GTB Bank

Sr. No.	Description	Mean	Std. Dev
1	The training content is providing a platform for technical skills.	3.81	0.917
2	The training content covered all necessary aspects of cyber security.	3.76	0.960
3	The training content was easy to understand.	3.71	0.915
4	The examples and case studies used were relevant to the job.	3.80	0.990
5	Training programs provide opportunities to update existing skills and acquire new technologies for employees in cyber security training	3.81	0.925
Overall Mean Scores		**3.78**	

Source: Survey Results (2024)

According to Table (4.7), respondents on the training content for the cyber security training course in GTB bank. Among the individual items, "The training content was easy to understand" received the lowest mean score of 3.71. The overall mean score of 3.78 indicates that, on average, respondents agree with the significance and effectiveness of the training methods employed.

4.4.4 Cyber Security Training Methods

To assess employee perceptions of the cyber security training method at GTB Bank, the study presented five key statements: The training methods used for delivering cyber security training play a significant role and are helpful and practical for employees in the current workplace. The hands-on exercises provided a better understanding of cyber security practices. Using multimedia, such as videos and slides, significantly enhanced the learning experience. The pace of the training was appropriate for effective learning. Each statement was rated on a Likert scale from 1 to 5. The detailed mean values and standard deviations for these statements are presented in Table 4.8 below.

Table (4.8) Cyber Security Training Methods of GTB Bank

Sr. No.	Description	Mean	Std. Dev
1	The training methods used for delivering cyber security training play a significant role.	3.66	0.947
2	Cybersecurity training methods are helpful and practical for employees in the current workplace.	3.75	0.998
3	The hands-on exercises provided a better understanding of cyber security practices.	3.69	0.970
4	The use of multimedia, such as videos and slides, significantly enhanced the learning experience.	3.75	0.991
5	The pace of the training was appropriate for effective learning.	3.68	0.951
Overall Mean Scores		**3.70**	

Source: Survey Results (2024)

According to Table (4.8), respondents highlighted that the training methods for the cyber security training course at “Cybersecurity training methods are useful and practical for employees in the current workplace” and “Using multimedia, such as videos and slides, significantly enhanced the learning experience”, both of which had a mean score of 3.75. Conversely, respondents barely agreed that "The training methods used for delivering cyber security training play a significant role," with a minimum mean score of 3.66. The overall mean score of 3.70 indicates that, on average, respondents agree with the significance and effectiveness of the training methods employed.

4.4.5 Cyber Security Training Evaluation

The study evaluated employee views on cyber security training evaluation at GTB bank using five distinct statements: Regular evaluation of employee understanding of cyber security concepts is essential; the specifications used to evaluate the course are unbiased and fair; timely feedback was received on performance; the feedback provided during the training process helped identify areas for improvement. Each statement was rated on a Likert scale from 1 to 5. The detailed mean values and standard deviations for these statements are presented in Table 4.9 below.

Table (4.9) Cyber Security Training Evaluation

Sr. No.	Description	Mean	Std. Dev
1	Regular evaluation of employee understanding of cyber security concepts is essential.	3.73	0.880
2	The methods used to evaluate the course are unbiased and fair.	3.74	0.839
3	Timely feedback was received on performance during the training.	3.70	0.809
4	The feedback provided during the training was helpful.	3.82	0.875
5	The evaluation process helped identify areas for improvement.	3.78	0.874
Overall Mean Scores		**3.75**	

Source: Survey Results (2024)

According to Table (4.9), respondents particularly emphasized the training evaluation for the cyber security training course at GTB bank, noting that "The feedback provided during the training was helpful," which had a mean score of 3.82. Conversely, respondents barely agreed that "Timely feedback was received on performance during the training," with a minimum mean score of 3.70. The overall mean score of 3.75 indicates that respondents generally agree on the importance and effectiveness of the evaluation process used in the training program.

4.5 Descriptive Statistics for Employee Behavior and Work Performance

In this section, employee behaviors and work performance are measured. The specific items related to employee behaviors and work performance are detailed in Tables (4.10) and (4.11).

4.5.1 Employee Behavior

The study evaluated employees' views on behavior perception at GTB bank using five distinct statements: Regularly complying with cybersecurity protocols at work, promptly reporting suspicious activities or potential threats, encouraging colleagues to follow cybersecurity best practices, staying updated with the latest cybersecurity trends and practices, and assuming responsibility for maintaining cybersecurity within the organization. Each statement was rated on a Likert scale from 1 to 5. The detailed mean values and standard deviations for these statements are presented in Table (4.10) below.

Table (4.10) Employees Perception of Behavior

Sr. No.	Description	Mean	Std. Dev
1	Regularly complying with cyber security protocols at work.	3.87	0.932
2	Promptly reporting suspicious activities or potential threats.	3.87	0.892
3	Encouraging colleagues to follow cyber security best practices.	3.83	0.870
4	Remaining informed about the latest cybersecurity trends and practices.	3.94	0.907
5	Assuming responsibility for maintaining cyber security within the organization.	3.91	0.922
Overall Mean Scores		**3.88**	

Source: Survey Results (2024)

According to Table (4.10), respondents particularly emphasized the employee behavior for the cyber security training course at GTB bank, noting that " Remaining informed about the latest cybersecurity trends and practices," which had a mean score of 3.94. Conversely, respondents barely agreed that " Encouraging colleagues to follow cyber security best practices.," with a minimum mean score of 3.83. The overall mean score of 3.88 indicates that respondents generally agree on the importance and effectiveness of the employee behavior process used in the training program.

4.5.2 Employee Work Performance

The study evaluated employees' views on work performance perception at GTB bank using five distinct statements: The cybersecurity training has positively impacted overall work performance; the ability to solve cybersecurity-related issues has improved; there has been a reduction in cybersecurity mistakes or incidents at work; training makes employees more prepared to handle cybersecurity threats. Each statement was rated on a Likert scale from 1 to 5. The detailed mean values and standard deviations for these statements are presented in Table (4.11) below.

Table (4.11) Employees Perception of Work Performance

Sr. No.	Description	Mean	Std. Dev
1	The cyber security training has positively impacted overall work performance.	3.87	0.895
2	The ability to solve cyber security-related issues has improved.	3.83	0.870
3	Training has resulted in a reduction in cyber security mistakes or incidents at work.	3.78	0.968
4	Training makes employees more prepared to handle cybersecurity threats.	3.77	0.986
5	Positive feedback on work performance has been received since the training.	3.79	0.978
Overall Mean Scores		3.81	

Source: Survey Results (2024)

According to Table (4.11), respondents emphasized the impact of the cybersecurity training course at GTB Bank on employee work performance, particularly noting that "the cybersecurity training has positively impacted my overall work performance," which received a mean score of 3.87. Conversely, respondents barely agreed that " Training makes employees more prepared to handle cybersecurity threats," with a minimum mean score of 3.77. The overall mean score of 3.81 indicates that respondents generally agree on the importance and effectiveness of the employee work performance process used in the training program.

Table (4.12) Overall Mean Score of Cybersecurity Training Practices

Sr. No.	Description	Mean	Std. Dev
1	Cyber Security Training Needs	3.82	0.802
2	Cybersecurity Training Objective	3.82	0.871
3	Cybersecurity Training Content	3.78	0.825
4	Cybersecurity Training Method	3.70	0.929
5	Cybersecurity Training Evaluation	3.75	0.814
6	Employee Behavior	3.88	0.862
7	Employee Work Performance	3.81	0.818

Source: Survey Results (2024)

The descriptive statistics from Table (4.12) provide valuable insights into the effectiveness of various aspects of cyber security training practices. Overall, the mean scores across different categories, such as Cyber Security Training Needs, Objectives, Content, Methods, and Evaluation, fall within a close range of 3.70 to 3.82, indicating a consistent and moderately high perception of their effectiveness. Notably, the highest mean score of 3.88 in Employee Behavior indicated that cyber security training significantly influences employees' security practices, enhancing awareness and responsible behavior.

Moreover, the positive impact of cyber security training extends to overall work performance, as indicated by a mean score of 3.81. This underscores the broader benefits of well-implemented training programs, which not only foster a secure working environment but also enhance overall work performance. These statistics emphasize the need for continuous improvement in training content, methods, and evaluation processes to maximize the benefits of cyber security training.

4.6 Analysis on the Effect of Cyber Security Training Practices on Employee Behavior

The connection between the independent and dependent variables was investigated using multiple regression analysis. Table (4.13) displays the outcomes of this analysis. The study aimed to determine the connection between employee performance and essential banking training practices, including training needs, objectives, content, methods, and evaluation.

Table (4.13) The Effect of Cyber Security Training Practices on Employee Behavior

Variable	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	VIF
	B	Std. Error	β			
(Constant)	-0.065	0.154		-0.419	0.676	
Cyber Security Training Needs	0.782***	0.083	0.727	9.381	0.000	8.726
Cyber Security Training Objective	0.127	0.083	0.128	1.535	0.127	10.148
Cyber Security Training Content	0.124**	0.056	0.119	2.225	0.028	4.139
Cyber Security Training Method	0.001	0.029	0.001	0.045	0.964	1.456
Training Evaluation	0.001	0.031	0.001	0.033	0.974	1.214
R Square	0.901					
Adjusted R Square	0.898					
F Value	262.037***					

Source: Survey Results (2024)

The outcome of the correlation reveals the impact of cyber security training practices on employee behavior. The constant term, with a coefficient of -0.065 and a significance level (Sig.) of 0.676, indicates that it is not statistically significant. This implies that when all independent variables are equal to zero, the predicted employee behavior is essentially negligible.

Cyber Security Training Needs (B = 0.782, β = 0.727, Sig. = 0.000) has a strong and significant positive effect on employee behavior, indicating this effect is highly significant. The Variance Inflation Factor (VIF) is 8.726, suggesting some correlation between predictors but generally acceptable.

Cyber Security Training Content (B = 0.124, β = 0.119, Sis. = 0.028) has a significant positive effect, although it is smaller. The VIF is 4.139, which is within acceptable limits.

Cyber Security Training Objective (B = 0.127, β = 0.128, Sig. = 0.127) is not statistically significant. Cyber Security Training Method (B = 0.001, β = 0.001, Sig. = 0.964) also lacks statistical significance, with a VIF of 1.456 indicating no concerns about predictor correlation. Similarly, Training Evaluation (B = 0.001, β = 0.001, Sig. = 0.974) is not statistically significant, and its VIF of 1.214 suggests no issues with predictor correlation.

According to Table 4.13, the R Square value is 0.901, and the Adjusted R Square value is 0.898. These values indicate that the model explains a significant proportion of the variance in employee behavior. The F Value of 262.037 signifies that the overall regression model is statistically significant, implying that the combined effect of the independent variables on employee behavior is substantial.

4.7 Analysis on the Effect of Employee Behavior on Employee Work Performance

This study examines the impact of employee behavior on employee work performance at GTB Bank using regression analysis. The regression analysis is presented in Table (4.14).

Table (4.14) The Effect of Employee Behavior on Employee Work Performance

Variable	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	VIF
	B	Std. Error	β			
(Constant)	0.504***	0.137		3.686	0.000	
Work Performance	0.851***	0.034	0.897	24.719	0.000	1.000
R Square	0.805					
Adjusted R Square	0.804					
F Value	611.045***					

Source: Survey Results (2024)

According to the table (4.14) The regression analysis offers important insights into the relationship between employee behavior and work performance at GTB Bank. The analysis reveals that the coefficient for work performance is 0.851, a standardized coefficient (β) of 0.897. A strong positive relationship in standardized terms

The R Square value of 0.805 indicates that 80.5% of the variance in work performance can be explained by employee behavior, with an Adjusted R Square of 0.804 confirming a strong model fit. The F Value of 611.045 further signifies that the overall regression model is statistically significant, underscoring the substantial influence of employee behavior on work performance. Additionally, the Variance Inflation Factor (VIF) for work performance is 1.000, indicating no multicollinearity issues and suggesting that the predictor variable provides reliable estimates.

CHAPTER V
CONCLUSION

This chapter includes three main parts of the study. The first part is findings and discussions from previous chapters. Following, the second part is suggestions and recommendations based on the study’s findings. The final part is the limitations, and the need for further research on employee work performance. Therefore, the findings based on the research objectives which guided the study are summarized below.

5.1 Finding and Discussion

This study examines the cybersecurity training practices provided by Global Treasure Bank and the effect of cybersecurity training practices on employee work performance at Global Treasure Bank. The data were collected using structured questionnaires based on a five-point Likert scale, distributed to a sample of 150 employees, including IT managers and staff, random selected from 150 branches of GTB Bank in Myanmar.

A demographic survey of 150 employees at Global Treasure Bank shows that 65% are female and 35% are male. The majority of the employees are aged between 26 and 45 years (74%), and most hold graduate degrees (71%). Job roles vary widely, ranging from Junior/Senior Assistants (38%) to Managers/Assistant Managers (30%). Experience levels are balanced, with groups having 4-6 years and over ten years of experience (23%).

The pervasive nature of cyber threats in the digital landscape necessitates a robust response from organizations, particularly financial institutions, that handle sensitive customer data and transactions. GTB Bank, like many others in the sector, faces the dual challenge of ensuring robust cybersecurity measures while maintaining high employee work performance.

According to the survey results, this study indicates a positive relationship between cybersecurity training and employee work performance at GTB bank. Quantitative analysis revealed that employees who participated in comprehensive training programs reported higher levels of performance levels, as measured by their ability to identify and mitigate security threats, adherence to security protocols, and overall job efficiency.

The positive effect between cybersecurity training and employee performance supports assertions about the essential role of training in enhancing security awareness and operational efficiency. The effect of training on employee performance underscores the necessity for continuous investment in employee development programs. For GTB bank, these findings suggest that enhancing the scope and depth of cybersecurity training can lead to substantial improvements in employee work performance, prove IT knowledge, best practices, and overall security posture, offering a competitive advantage in the increasingly digital financial landscape.

5.2 Suggestion and Recommendation

Based on the findings of the study, the following are some suggestions and recommendations to enhance employee work performance. This study investigated how GTB bank employees performed in relation to cybersecurity training practices, including needs, objectives, methods, and evaluation.

GTB bank should consider expanding the scope of cybersecurity training to cover emerging threats and technologies. Training modules could include simulations and real-life scenarios to better prepare employees for handling complex security challenges. Recognizing the diverse job roles within the organization, GTB bank should customize training programs to address specific cybersecurity needs relevant to different departments and levels of responsibility.

Implementing a culture of continuous learning is essential. GTB bank should encourage employees to stay updated with ongoing refresher courses, webinars, and certifications in cybersecurity to maintain high levels of awareness and competence. Linking cybersecurity training outcomes with performance evaluation metrics can incentivize employees to engage in training activities actively. Recognizing and rewarding employees who excel in security practices can reinforce positive behavior.

Alongside training, GTB bank should invest in advanced cybersecurity tools and technologies that complement employee skills. This includes regular updates to the security software and tools used across the organization. Beyond formal training sessions, GTB bank should promote a security-conscious culture where cybersecurity is everyone's responsibility. Encouraging open communication channels for reporting potential threats and fostering collaboration on security initiatives can strengthen security posture. By implementing these recommendations, GTB Bank can improve employee work performance but also strengthen its ability to withstand cyber threats, thereby protecting customer data and maintaining trust in the digital financial landscape.

5.3 Needs for Further Study

This study offers valuable insights into the relationship between cybersecurity training and employee work performance at Global Treasure Bank. Several avenues for further research are identified. Conducting studies to observe the long-term effects of cybersecurity training on employee performance could provide a deeper understanding of sustainability and effectiveness over time. Comparing the effectiveness of different cybersecurity training methods (e.g., online courses vs. in-person workshops) on employee performance across various organizational contexts could reveal optimal approaches. Extending the research to include comparative analysis with other sectors beyond financial institutions could offer broader insights into the transferability of cybersecurity training practices and their impact on employee performance. Investigating external factors such as regulatory changes technological advancements, and evolving cyber threats that may influence the effectiveness of cybersecurity training and its impact on employee performance. Examining how cybersecurity training initiatives influence organizational culture, particularly in terms of attitudes towards security responsibilities and collaboration across departments. Conducting a comprehensive cost-benefit analysis of cybersecurity training investments, including both direct and indirect benefits (e.g., reduced security incidents, enhanced customer trust), to justify resource allocations.

Addressing these areas of further study could enhance the depth and applicability of findings related to cybersecurity training practices and their impact on employee work performance, thereby contributing to more effective cybersecurity strategies within GTB bank and similar organizations.

REFERENCES

Adams, R. (2022). The role of compliance in financial institutions. *Financial Times*.

Adams, S., & Clark, E. (2021). Evaluating training and development programs. *Journal of Business Research*, 56(3), 198-213.

Afsana, J. O. B. A. Y. R. A., Afrin, F. A. R. H. A. N. A., & Tarannum, T. A. S. N. E. E. M. (2016). Effect of training on employee performance: An empirical study on telecommunication industry in Bangladesh. *Journal of Business and Technology (Dhaka)*, *10*(2), 67-80.

Aguinis, H., & Kraiger, K. (2009). Benefits of training and development for individuals and teams, organizations, and society. *Annual Review of Psychology*, 60, 451-474.

Amir Elnaga, & Amen Imran. (2013). The effect of training on employee performance. *European Journal of Business and Management, 5*(4), 2222-1905.

Anderson, M., et al. (2019). Effective training practices. *Journal of Organizational Behavior*, *34*(4), 321-336.

Armstrong, M., & Taylor, S. (2023). Armstrong's handbook of human resource management practice: A guide to the theory and practice of people management.

Athar, R., & Shah, F. M. (2015). Impact of training on employee performance (banking sector Karachi). *IOSR Journal of Business and Management*, *17*(11), 58-67.

Best, J. W. (1977). *Research in education* (3rd ed.). New Jersey: Prentice Hall.

Bosworth, S., & Kabay, M. E. (Eds.). (2002). *Computer security handbook*. John Wiley & Sons.

Brown, A., & White, B. (2019). Enhancing cyber security through effective employee training. *Journal of Information Security*, *15*(2), 45-61.

Buckley, R., & Caple, J. (2004). *The theory and practice of training*.

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.

Chen, J. V., Li, Y., Bao, Y., & Huang, Y. (2020). Cybersecurity and human factors: A research agenda. *Computers & Security, 94*, 101894.

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

Demetra, L., Lauren, J., John, C., & Carolyn, S. (2008). *Human Resource Management*. Pearson Education.

Elnaga, A., & Imran, A. (2013). The effect of training on employee performance. *European Journal of Business and Management*, *5*(4), 137-147.

Gebrehiwot, G. D., & Elantheraiyan, P. (2023). A study on the effect of training on employee performance in the case of Mekelle City, Tigray, Ethiopia. *Social Sciences & Humanities Open*, *8*(1), 100567.

Ghosh, S., & Goswami, S. (2020). Human resource development: A strategic approach. *SAGE Publications India*.

Ghuman, K. (2010). Management: Concepts, practice & cases. Tata McGraw-Hill Education.

Green, P. (2019). Employee development in the financial sector. *Banking Review Quarterly*, *89*(2), 99-115.

Hasan, M. T. (2023). Cybersecurity in bank: a case on employee engagement and responsibility for a Secure Digital Environment (SDE) in the selected branch.

Hashim, M., Khan, M. A., & Syeed, T. (2014). The impact of training and development on employees performance and productivity: A case study of United Bank Limited Peshawar City, KPK, Pakistan.

Huang, J., & Knight, A. P. (2017). "Resources and relationships in entrepreneurship: An exchange theory of the development and effects of the entrepreneurial team." *Academy of Management Review*, *42*(1), 80-102.

Johnson, C., Anderson, D., & Davis, E. (2020). The impact of cyber security training on employee behavior: A case study of banking institutions. *Security Management Journal*, *8*(3), 112-128.

Jones, M. (2021). Enhancing employee productivity. *Journal of Organizational Behavior*, *42*(4), 367-380.

Jones, R., & Brown, K. (2021). Employee training and development: Concepts, practices, and implications for organizational behavior. *Journal of Applied Psychology*, *25*(4), 321-335.

Jones, T. E. (2019). Key factors that influence job performance: The performance pathway model. *Training Industry*.

Kaspersky, I. C. S. (2021). Threat landscape for industrial automation systems. *Statistics for H*, 1, 2021.

Kim, S. (2017). Training for cybersecurity in the workplace. *Cybersecurity Journal*, *12*(2), 123-137.

Kirkpatrick, D. L. (1956). How to start an objective evaluation of your training program. Journal of the American Society of Training Directors, *10*(3), 18-22.

Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating training programs: The four levels* (3rd ed.). Berrett-Koehler Publishers.

Kirkpatrick, J. D., & Kirkpatrick, W. K. (2016). *Kirkpatrick's four levels of training evaluation*. Association for Talent Development.

Lee, H. (2021). Impact of security training on employee performance. *Journal of Business Research*, *56*(1), 75-89.

Mamoria, C. B. (1995). *Personnel Management*. Himalaya Publishing House.

Noe, R. A. (2020). *Employee training and development* (8th ed.). McGraw-Hill Education.

Reio, T. G., Jr., & Callahan, J. L. (2004). "Aiming for More Effective Learning, Teaching, and Development Through Understanding, Applying, and Evaluating the Kirkpatrick Model." *Performance Improvement*, *43*(3), 8-13.

Robbins, S. P., & Judge, T. A. (2019). *Essentials of organizational behavior*. Pearson.

Smith, J. (2018). The essentials of training. *Training Journal*, *45*(3), 22-27.

Smith, J. (2020). *Performance management in organizations*. McGraw-Hill.

Smith, J. (2023). Cyber security training practices in banking: Impact on employee behavior and organizational performance. *International Journal of Cyber Security*, *7*(1), 55-72.

Taylor, D. (2020). Resilience through training. *Organizational Dynamics*, *49*(3), 213-225.

Taylor, L. (2017). Planning and implementing training programs. *Human Resource Management Review*, *28*(1), 45-58.

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

White, L. (2018). Cybersecurity and organizational performance. *International Journal of Information Security*, *17*(3), 199-210.

Yozi, N. A. (2018). Impact of training and development of academics in an institution of higher learning: a case study of a University of Technology. *Business & Social Sciences Journal*, *3*(2), 70-89.

APPENDIX A

SURVEY QUESTIONNAIRE

CYBERSECURITY TRAINING PRACTICES ON EMPLOYEE WORK PERFORMANCE AT GLOBAL TREASURE BANK

Dear Participant,

I am Hnin Yu Wai, currently attending the Master of Banking and Finance program at Yangon University of Economics. As part of my thesis titled "Cybersecurity Training Practices on Employee Work Performance at Global Treasure Bank," I am conducting a survey to gather insights on the impact of cybersecurity training on employee performance within our organization. Your participation is crucial in helping us understand how training programs can be optimized to enhance work performance and ensure robust cybersecurity practices. The survey will take approximately 10 days to complete, and your responses will be kept confidential and used solely for academic purposes.

Thank you for taking the time to participate in this survey. Your input is invaluable to my research and will contribute significantly to the understanding and improvement of cybersecurity training practices at Global Treasure Bank.

Your cooperation and support are greatly appreciated.

Sincerely,
Hnin Yu Wai

Master of Banking and Finance Student

Yangon University of Economics

Section 1: Demographic Information

1. Age

18-25 □

26-35 □

36-45 □

46-55 □

56 and above □

2. Gender

Male □

Female □

3. Education Level

Under Graduate □

Graduate □

Master Degree □

Doctor Degree □

Other □

4. Job Level

Entry-level □

Junior-level □

Senior-level □

Executive □

Other(please specify) □

5. Years of Experience at GTB

Less than 1 year □

1-3 years □

4-6 years □

7-10 years □

More than 10 years □

APPENDIX B

This section is focused on measuring employee perceptions within Global Treasure Bank. The scale that was used in this item was an interval scale. In particular, the respondents were asked to rate on a 5-point Liker scale their perceptions and opinions with respect to the statements, with 1= strongly disagree and 5= strongly agree.

Section 2: Training Practices

Part I: Cyber Security Training Needs

Sr. No.	Particular	1	2	3	4	5
1	Training programs are necessary to enhance employee ability. ဝန်ထမ်းများ၏ စွမ်းရည်မြှင့်တင်ရန် လေ့ကျင့်ရေး အစီအစဉ်များ လိုအပ်ပါသည်။					
2	Cyber security training is essential needed to protect the digital infrastructure of the bank. ဘဏ်၏ ဒစ်ဂျစ်တယ်အခြေခံအဆောက်အအုံကို ကာကွယ်ရန်အတွက်ဆိုက်ဘာလုံခြုံရေးသင်တန်းသည် မရှိမဖြစ်လိုအပ်ပါသည်။					
3	Training needs involve identifying cyber security skills and knowledge gaps among employees. လေ့ကျင့်ရေးလိုအပ်ချက်များတွင် ဝန်ထမ်းများအကြား ဆိုက်ဘာလုံခြုံရေးကျွမ်းကျင်မှုနှင့် အသိပညာကွာဟချက်များကို ခွဲခြားသတ်မှတ်ခြင်း ပါဝင်သည်။					
4	It is necessary that training programs be modified to meet the actual needs. အမှန်တကယ်လိုအပ်ချက်များနှင့် ကိုက်ညီစေရန် လေ့ကျင့်ရေးအစီအစဉ်များကို ပြုပြင်ပြောင်းလဲရန် လိုအပ်ပါသည်။					
5	GTB Bank employees are required to complete cyber security training. GTB ဘဏ်ဝန်ထမ်းများသည် ဆိုက်ဘာလုံခြုံရေး သင်တန်းကို ပြီးမြောက်ရန် လိုအပ်ပါသည်။					

Part II: Cyber Security Training Objective

Sr. No.	Particular	1	2	3	4	5
1	The cybersecurity training objectives were clearly defined. ဆိုက်ဘာလုံခြုံရေးသင်တန်း ရည်မှန်းချက်များကို ရှင်းရှင်းလင်းလင်းသတ်မှတ်ထားပါသည်။					
2	The objectives of cybersecurity training are to understand security issues and to act responsibly. ဆိုက်ဘာလုံခြုံရေးသင်တန်း၏ ရည်ရွယ်ချက်မှာ လုံခြုံရေးဆိုင်ရာ ပြဿနာများကို နားလည်ရန်နှင့် တာဝန်သိစွာ လုပ်ဆောင်ရန်ဖြစ်သည်။					
3	The cybersecurity training objectives helped understand the importance of cybersecurity. သင်တန်းရည်ရွယ်ချက်များသည် ဆိုက်ဘာလုံခြုံရေး၏အရေးပါပုံကို နားလည်သဘောပေါက်စေခဲ့သည်။					
4	The cybersecurity training objectives at GTB Bank aligned well with employee work competency. GTB ဘဏ်၏ ဆိုက်ဘာလုံခြုံရေးသင်တန်း ရည်ရွယ်ချက်များသည် ဝန်ထမ်းများ၏အလုပ်ကျွမ်းကျင်မှုနှင့် ကောင်းမွန်စွာကိုက်ညီပါသည်။					
5	The cybersecurity objectives are to identify and effectively mitigate potential cyber threats. ဆိုက်ဘာလုံခြုံရေး ရည်ရွယ်ချက်များသည် ဖြစ်နိုင်ချေရှိသော ဆိုက်ဘာခြိမ်းခြောက်မှုများကို ဖော်ထုတ်ရန်နှင့် ထိထိရောက်ရောက် လျှော့ပါးစေရန်ဖြစ်သည်။					

Part III: Cyber Security Training Content

Sr. No.	Particular	1	2	3	4	5
1	The training content is providing a platform for technical skills. သင်တန်းအကြောင်းအရာသည် နည်းပညာပိုင်းဆိုင်ရာ ကျွမ်းကျင်မှုများအတွက် ပလက်ဖောင်းတစ်ခုဖြစ်သည်။					
2	The training content covered all necessary aspects of cybersecurity. သင်တန်းအကြောင်းအရာသည် ဆိုက်ဘာလုံခြုံရေး၏ လိုအပ်သောကဏ္ဍအားလုံးကို အကျုံးဝင်သည်။					
3	The training content was easy to understand. သင်တန်းအကြောင်းအရာသည် နားလည်ရလွယ်ကူသည်။					
4	The examples and case studies used were relevant to the job. နမူနာများနှင့် ဖြစ်ရပ်လေ့လာမှုများသည် အလုပ်နှင့် သက်ဆိုင်သည်။					
5	Training programs provide opportunities to update existing skills and acquire new technologies for employees in cybersecurity training သင်တန်းပရိုဂရမ်များသည် ဆိုက်ဘာလုံခြုံရေးသင်တန်းတွင် ဝန်ထမ်းများအတွက် ရှိပြီးသားအရည်အချင်းများကို မွမ်းမံရန်နှင့် နည်းပညာအသစ်များရယူရန် အခွင့်အလမ်းများကို ပေးသည်။					

Part IV: Cyber Security Training Methods

Sr. No.	**Particular**	**1**	**2**	**3**	**4**	**5**
1	The training methods used for delivering cybersecurity training play a significant role. ဆိုက်ဘာလုံခြုံရေးသင်တန်းပို့ချရာတွင်အသုံးပြုသည့်လေ့ကျင့်ရေးနည်းလမ်းများသည် အရေးပါသောအခန်းကဏ္ဍမှပါဝင်သည်။					
2	Cybersecurity training methods are helpful and practical for employees in the current workplace. ဆိုက်ဘာလုံခြုံရေးလေ့ကျင့်ရေးနည်းလမ်းများသည်လက်ရှိလုပ်ငန်းခွင်ရှိဝန်ထမ်းများအတွက် အသုံးဝင်ပြီးလက်တွေ့ကြပါသည်။					
3	The hands-on exercises provided a better understanding of cybersecurity practices. လက်ဆင့်ကမ်းလေ့ကျင့်ခန်းများသည် ဆိုက်ဘာလုံခြုံရေးအလေ့အကျင့်များကို ပိုမိုကောင်းမွန်စွာနားလည်စေပါသည်။					
4	The use of multimedia, such as videos and slides, significantly enhanced the learning experience. ဗီဒီယိုများနှင့် ဆလိုက်များကဲ့သို့သော မာလ်တီမီဒီယာကို အသုံးပြုခြင်းသည် သင်ယူမှုအတွေ့အကြုံကို သိသိသာသာ တိုးတက်စေသည်။					
5	The pace of the training was appropriate for effective learning. သင်တန်း၏အရှိန်အဟုန်သည် ထိရောက်သောသင်ယူမှုအတွက် သင့်လျော်ပါသည်။					

Part V: Cyber Security Training Evaluation

Sr. No	Particular	1	2	3	4	5
1	Regular evaluation of employee understanding of cybersecurity concepts is essential. ဆိုက်ဘာလုံခြုံရေး သဘောတရားများကို ဝန်ထမ်းများ နားလည်သဘောပေါက်မှုကို ပုံမှန်အကဲဖြတ်ရန် အရေးကြီးပါသည်။					
2	The methods used to evaluate the course are unbiased and fair. သင်တန်းကို အကဲဖြတ်ရန် အသုံးပြုသည့် နည်းလမ်း များသည် ဘက်မလိုက်ဘဲ မျှတသည်။					
3	Timely feedback was received on performance during the training. သင်တန်းကာလအတွင်း စွမ်းဆောင်ရည်အပေါ် အချိန် နှင့်တစ်ပြေးညီ တုံ့ပြန်ချက်ရရှိခဲ့ပါသည်။					
4	The feedback provided during the training was helpful. သင်တန်းကာလအတွင်း ပေးထားသော အကြံပြုချက် သည် အထောက်အကူဖြစ်စေပါသည်။					
5	The evaluation process helped identify areas for improvement. အကဲဖြတ်ခြင်းလုပ်ငန်းစဉ်သည် တိုးတက်မှုအတွက် နယ်ပယ်များကို ဖော်ထုတ်ရာတွင် အထောက်အကူ ဖြစ်စေသည်။					

Section 3: Employee Behavior and Employee Work Performance

Part I: Employee Behavior

Sr. No.	Particular	1	2	3	4	5
1	Regularly complying with cyber security protocols at work. အလုပ်တွင် ဆိုက်ဘာလုံခြုံရေး ပရိုတိုကောများကို ပုံမှန်လိုက်နာပါသည်။					
2	Promptly reporting suspicious activities or potential threats. သံသယဖြစ်ဖွယ် လှုပ်ရှားမှုများ သို့မဟုတ် ဖြစ်နိုင်ချေရှိသော ခြိမ်းခြောက်မှုများကို ချက်ချင်းသတင်းပို့ပါသည်။					
3	Encouraging colleagues to follow cyber security best practices. ဆိုက်ဘာလုံခြုံရေး အကောင်းဆုံးအလေ့အကျင့်များကို လိုက်နာရန် လုပ်ဖော်ကိုင်ဖက်များအား တိုက်တွန်းပါသည်။					
4	Remaining informed about the latest cybersecurity trends and practices. နောက်ဆုံးပေါ်ဆိုက်ဘာလုံခြုံရေးလမ်းကြောင်းများနှင့် အလေ့အကျင့်များဖြင့် အပ်ဒိတ်လုပ်နေပါ။					
5	Assuming responsibility for maintaining cyber security within the organization. အဖွဲ့အစည်းအတွင်း ဆိုက်ဘာလုံခြုံရေးကို ထိန်းသိမ်းရန် တာဝန်ရှိသည်။					

Part II: Employee Work Performance

Sr. No.	Particular	1	2	3	4	5
1	The cyber security training has positively impacted overall work performance. ဆိုက်ဘာလုံခြုံရေးသင်တန်းသည် လုပ်ငန်းတစ်ခုလုံး၏ စွမ်းဆောင်ရည်အပေါ် သက်ရောက်မှုရှိသည်။					
2	The ability to solve cyber security-related issues has improved. ဆိုက်ဘာလုံခြုံရေးနှင့်ပတ်သက်သည့် ပြဿနာများကို ဖြေရှင်းနိုင်စွမ်း တိုးတက်လာခဲ့သည်။					
3	Training has resulted in a reduction in cyber security mistakes or incidents at work. သင်တန်းသည် လုပ်ငန်းခွင်တွင် ဆိုက်ဘာလုံခြုံရေးအမှားများ သို့မဟုတ် အဖြစ်အပျက်များကို လျှော့ချပေးသည်။					
4	Training makes employees more prepared to handle cybersecurity threats. သင်တန်းပေးခြင်းသည် ဝန်ထမ်းများအား ဆိုက်ဘာလုံခြုံရေးခြိမ်းခြောက်မှုများကို ကိုင်တွယ်ရန် ပိုမိုအဆင်သင့်ဖြစ်စေသည်။					
5	Positive feedback on work performance has been received since the training. သင်တန်းချိန်မှစ၍ လုပ်ငန်းစွမ်းဆောင်ရည်အပေါ် အပြုသဘောဆောင်သော အကြံပြုချက်များကို လက်ခံရရှိခဲ့ပါသည်။					

APPENDIX C
REGRESSION ANALYSIS

The Effect of Cyber Security Training Practices on Employee Behavior

Notes

Output Created		21-JUN-2024 23:04:28
Comments		
Input	Data	C:\Users\Hnin Yu Wai\Desktop\Ma Hnin (SPSS)Out Put\Untitled1.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	150
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.
Syntax		REGRESSION /DESCRIPTIVES MEAN STDDEV CORR SIG N /MISSING LISTWISE /STATISTICS COEFF OUTS CI(95) R ANOVA COLLIN TOL CHANGE ZPP /CRITERIA=PIN(.05) POUT(.10) /NOORIGIN /DEPENDENT EBMean /METHOD=ENTER CTNMean CTOMean CTCMean CTMMean CTEMean /RESIDUALS DURBIN /CASEWISE PLOT(ZRESID) OUTLIERS(3).
Resources	Processor Time	00:00:00.05
	Elapsed Time	00:00:00.19
	Memory Required	6720 bytes
	Additional Memory Required for Residual Plots	0 bytes

Regression

Descriptive Statistics

	Mean	Std. Deviation	N
Employee Behavior	3.88	0.862	150
Cyber Security Training Needs	3.82	0.802	150
Cybersecurity Training Objective	3.82	0.871	150
Cybersecurity Training Content	3.78	0.825	150
Cybersecurity Training Method	3.70	0.929	150
Cybersecurity Training Evaluation	3.75	0.814	150

Model Summary[b]

					Change Statistics					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.949[a]	0.901	0.898	0.276	0.901	262.037	5	144	0.000	1.937

a. Predictors: (Constant), Cybersecurity Training Evaluation, Cybersecurity Training Content, Cybersecurity Training Method, Cyber Security Training Needs, Cybersecurity Training Objective

b. Dependent Variable: Employee Behavior

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	99.848	5	19.970	262.037	.000[b]
	Residual	10.974	144	0.076		
	Total	110.822	149			

a. Dependent Variable: Employee Behavior

b. Predictors: (Constant), Cybersecurity Training Evaluation, Cybersecurity Training Content, Cybersecurity Training Method, Cyber Security Training Needs, Cybersecurity Training Objective

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	-0.065	0.154		-0.419	0.676	-0.369	0.240					
	Cyber Security Training Needs	0.782	0.083	0.727	9.381	0.000	0.617	0.947	0.944	0.616	0.246	0.115	8.726
	Cybersecurity Training Objective	0.127	0.083	0.128	1.535	0.127	-0.037	0.290	0.908	0.127	0.040	0.099	10.148
	Cybersecurity Training Content	0.124	0.056	0.119	2.225	0.028	0.014	0.234	0.823	0.182	0.058	0.242	4.139
	Cybersecurity Training Method	0.001	0.029	0.001	0.045	0.964	-0.057	0.059	0.301	0.004	0.001	0.687	1.456
	Cybersecurity Training Evaluation	0.001	0.031	0.001	0.033	0.974	-0.059	0.061	0.151	0.003	0.001	0.823	1.214

a. Dependent Variable: Employee Behavior

The Effect of Employee Behavior on Employee Work Performance

```
REGRESSION
  /DESCRIPTIVES MEAN STDDEV CORR SIG N
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS CI(95) BCOV R ANOVA COLLIN TOL CHANGE ZPP
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT EWPMean
  /METHOD=ENTER EBMean
  /RESIDUALS DURBIN
  /CASEWISE PLOT(ZRESID) OUTLIERS(3).
```

Regression

Descriptive Statistics

	Mean	Std. Deviation	N
Employee Work Performance	3.81	0.818	150
Employee Behavior	3.88	0.862	150

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.897[a]	0.805	0.804	0.362	0.805	611.045	1	148	0.000	2.242

a. Predictors: (Constant), Employee Behavior

b. Dependent Variable: Employee Work Performancee

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	80.172	1	80.172	611.045	.000[b]
	Residual	19.418	148	0.131		
	Total	99.590	149			

a. Dependent Variable: Employee Work Performancee

b. Predictors: (Constant), Employee Behavior

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	0.504	0.137		3.686	0.000	0.234	0.775					
	Employee Behavior	0.851	0.034	0.897	24.719	0.000	0.783	0.919	0.897	0.897	0.897	1.000	1.000

a. Dependent Variable: Employee Work Performancee