ADDIS ABABA UNIVERSITY

COLLEGE OF BUSINESS AND ECONOMICS

MASTER OF BUSINESS INFORMATION SYSTEMS (MBIS)

FACTORS AFFECTING INFORMATION SYSTEM SECURITY AWARENESS AMONG NIB BANK EMPLOYEES: KNOWLEDGE, ATTITUDE, PERCEPTION AND TRAINING -BASED ANALYSIS

By: LUDANA YOHANNES

June , 2024

Addis Ababa, Ethiopia

FACTORS AFFECTING INFORMATION SECURITYAWARENESS AMONG NIB BANK EMPLOYEES: KNOWLEDGE, ATTITUDE, PERCEPTION AND TRAINING -BASED ANALYSIS

A Thesis Submitted to Addis Ababa University School of commerce in Partial Fulfillment of the Requirement of the Degree of Master of business information system

Adviser: Hailay Beyene(Ph.D.)

By: LUDANA YOHANNES

FACTORS AFFECTING INFORMATION SECURITYAWARENESS AMONG NIB BANK EMPLOYEES: KNOWLEDGE, ATTITUDE, PERCEPTION AND TRAINING -BASED ANALYSIS

A Thesis Submitted to Addis Ababa University School of commerce in Partial Fulfillment of the Requirement of the Degree of Master of business information system

By: Ludana Yohannes

Name and Signature of Members of the Examining Board

Hailay Beyene (Ph.D)	_____	_____
Advisor	Signature	Date
Melkamu Beyene (Ph.D)	_____	_____
Examiner	Signature	Date
Eyob Nigussie (Ph.D)	_____	_____
Examiner	Signature	Date

DECLARATION

This is to certify that the thesis prepared by LudanaYohannes, entitled: factors affecting information system security awareness among bank employees: knowledge, attitude, perception and training -based analysis and submitted in partial fulfillment of the requirements for master's degree in business information systems complies with the regulations of the university and meets the accepted standard with respect to originality and quality.

Researcher Name	**Signature**	**Date**
Ludana Yohannes		June, 2024

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to God for His unwavering guidance and strength throughout this journey. To my family, whose love and support have been a constant source of encouragement, thank you for believing in me. I am especially grateful to my advisor, Hailay Beyene (Ph.D.) for your invaluable mentorship, patience, and insightful feedback. This thesis would not have been possible without your dedication

LUDANA YOHANNES

June, 2024

ADDIS ABABA, ETHIOPIA

Contents

LIST OF TABLE

LIST OF ABBREVATIONS

DOS Denial of service

IBM International mortgage bankers

ISP Internet service provider

IT Information technology

ITU International Telecommunication Union

NBE The National Bank of Ethiopia

NIB Nib International Bank

SQL structured query language

WAN wide area network

XSS cross-site scripting

K knowledge

P perception

A Attitude

T Training

ABSTRACT

Financial institutions are often targeted by cyber-attacks, underscoring the importance of information security awareness among bank employees. This dissertation delves into the reasons behind the lack of awareness among NIB bank employees, exploring the relationship between employee knowledge, attitudes, perceptions of security threats, and the efficacy of training initiatives.

The researcher adopted a quantitative research methodology, utilizing numerical data collection and analysis to explain the phenomenon of information security awareness within the bank. The study focused on identifying the factors influencing information security awareness, including employee knowledge, attitudes, perceptions of threats, and the effectiveness of training programs.

Data was gathered through a survey administered to NIB bank employees, enabling the acquisition of quantitative insights into employee knowledge, attitudes, perceptions, and the perceived impact of training efforts. Subsequent analysis centered on examining the correlations between these factors and their contributions to information security awareness.

The primary objectives of the study were to pinpoint the key influencers of information security awareness, scrutinize the connections between knowledge, attitudes, perceptions, and training efficacy, and assess the influence of training programs on employee awareness.

The research outcomes aimed to offer actionable insights for banks to enhance their information security awareness initiatives. The results indicated that employees' limited awareness stemmed from moderate knowledge levels, negative attitudes, perceptions of threats, and insufficiently targeted training. By comprehending the factors shaping employee behaviors concerning information security, banks could fortify their defenses and safeguard customer and data assets effectively.

Keywords: Information Security Awareness, Bank Employees, Knowledge, Attitude, Perception, Training

Chapter one

Introduction

1.1 Background of the study

The internet's widespread public availability in the 1960s revolutionized interaction, making online transactions the norm (Abbate, 2000). Today, activities like buying and selling, bill payments, utility services, and even gas refills are conducted online across all industries, with healthcare, government, commercial, and banking sectors relying heavily on internet connectivity (Abbate, 2000). This dependence is particularly strong within the banking sector, where internet outages would significantly hinder functionality. However, despite the convenience of the digital age, information system security breaches have become increasingly common across industries. These breaches, defined as unauthorized access to a computer system, network, or database, can occur due to weak passwords, unpatched vulnerabilities, or human error (Angst et al., 2017). Their goals can be to gain access to sensitive information or disrupt the system itself. The targeted information or data can be personal or organization-specific (Angst et al., 2017).

Information security breaches are especially prevalent in the banking sector due to the vast amount of sensitive customer information held by these institutions. This makes them prime targets for cybercriminals who employ tactics like identity theft, phishing, malware, tricking employees or customers into revealing credentials, and hacking to steal data (Angst et al., 2017; Zafar et al., 2016). These breaches not only pose a threat to banks but also erode customer trust and cause significant financial losses. Additionally, a damaged reputation can hinder customer acquisition and loyalty (Zafar et al., 2016). Studies by Accenture (2020) reveal that the average information security breach for financial service companies costs a staggering $13 million.

To effectively prevent information security breaches, banks must implement robust security measures. These can include multi-factor authentication, real-time email or text alerts, data encryption, and customer awareness campaigns regarding security breaches and control mechanisms. However, the most crucial element is employee education and training (Pollock, 2017). While numerous factors contribute to information security breaches, human error remains the most common culprit (Pollock, 2017). This includes inadequate security awareness, insufficient knowledge, negative attitudes towards security protocols, a lack of training, and a low perception of risk (Pollock, 2017). Measuring the true impact of information security breaches is often challenging due to potential overestimations or underestimations of associated costs.

The consequences of such breaches can be devastating for banks. Data breaches can expose sensitive customer information like account details, social security numbers, or credit card information (Angst et al., 2017). This can lead to significant financial losses for both the bank and its customers, who may face identity theft or fraudulent charges. Additionally, compromised employee credentials can allow criminals access to online banking systems, enabling fraudulent transactions (Zafar et al., 2016). These incidents not only result in direct financial losses but also erode customer trust, potentially damaging the bank's reputation for years to come (Zafar et al., 2016).

Being aware of information system security is crucial for maintaining cyber-security within a bank. As cyber threats become more frequent and complex imperative for organizations to ensure that their employees are well-informed and alert about potential security risks. However, despite the implementation of security policies and training programs, many employees still lack the necessary awareness regarding information system security. This knowledge gap poses a significant challenge to organizations, as it increases the likelihood of security breaches and data compromises (Siponen et al., 2010).

Recognizing the causes of employees' limited knowledge about information system security is essential for creating successful approaches to reduce security threats. Various elements may be responsible for this lack of awareness. Furthermore, the culture of the organization, methods of communication, and the extent of support from management can also impact employees' understanding of information system security (Grrma, 2020).

Given the potential consequences of inadequate security awareness, such as data breaches, financial losses, and reputational damage, there is a pressing need to investigate the underlying factors contributing to employees' lack of awareness in information system security. By identifying these factors, organizations can tailor their security awareness programs to address specific challenges and improve overall cyber security posture (Tebekew,2013).

For a bank like NIB Bank in Ethiopia, protecting customer information and maintaining trust are paramount. Effective cyber security within banks heavily relies on the knowledge and ability of employees, particularly those at the branch level, to overcome security challenges. This is because most customer interactions occur at the branch level. While main offices often have more robust cyber security measures and experienced personnel, branch-level employees may require additional training (Girma, 2020).

Therefore, this study aims to explore and analyze the reasons why employees lack awareness in information system security within the NIB Bank. By gaining insights into these factors, the study seeks to provide valuable recommendations for enhancing information system security awareness among employees and ultimately strengthening organizational cyber security defenses.

1.2 statement of the problem

The rise of digital banking has undeniably transformed how financial institutions operate. However, this increased reliance on information systems introduces a critical challenge: ensuring their security. Employee awareness of information system security protocols plays a vital role in safeguarding sensitive financial data and protecting banks from cyber threats (Albrechtsen, Hovden, & Kydland, 2017).

Unfortunately, previous research paints a concerning picture. Studies have consistently highlighted a lack of adequate information system security awareness among bank employees, including those at NIB Bank (Girum, 2020).

Woretaw and Lessa (2012) concluded that the level of awareness among employees in the Ethiopian banking sector is inadequate. Similarly, a study by Milkayas et al. (2019) revealed that employees in banks lack awareness of information system security breaches. This lack of awareness poses security risks, leaving banks vulnerable to data breaches and cyber-attacks. Addressing this issue is crucial for safeguarding the integrity and confidentiality of customer information, given the highly sensitive nature of financial data entrusted to banks (Milkayas et al., 2019).

This deficiency in awareness poses significant risks to the security of organizational information systems, potentially leading to data breaches, financial losses, and reputational damage. However, the underlying reasons for employees' lack of awareness in information system security remain poorly understood. Therefore, this study aims to investigate and analyze the root cause factors contributing to employees' insufficient awareness of information system security within organizations. By identifying these factors, the study seeks to provide insights and recommendations for enhancing information system security awareness among NIB Bank employees, thereby improving overall cyber security resilience.

1.3 Objectives of Research

1.3.1. General objective

The general objective of this study is to understand factors affecting information system security awareness among NIB bank employees.

1.3.2 Specific Objective

To achieve this research aim, the following objectives are set:

- To evaluate the knowledge level of NIB Bank branch employees on information security breaches and their consequences.
- To assess the attitudes of NIB Bank branch employees towards information security protocols and reporting procedures.
- To analyze the effectiveness of current information security breach training programs for NIB Bank branch employees.
- To investigate the role of individual perceptions such as risk awareness and self-efficacy in shaping information security awareness at NIB Bank.
- To identify key factors contributing to information security awareness gaps among NIB Bank branch employees for targeted interventions.

1.4 Research Question

The research question is:

- What are the main reasons for NIB bank employees to lack awareness?

1.5 Hypothesis

Hypothesis 1: Knowledge does not significantly affect awareness.

Hypothesis 2: Perception does not significantly affect awareness.

Hypothesis 3: Attitude does not significantly affect awareness.

Hypothesis 4: Training does not significantly affect awareness.

1.6 Significance of the Study

Studying the causes of employees' unawareness of information security in banks is crucial for various reasons. Firstly, it enables banks to proactively mitigate risks by identifying the root causes of employees' lack of awareness. Understanding why employees may not be fully informed about security protocols allows institutions to implement targeted interventions that strengthen their security posture and prevent potential breaches. This proactive approach is essential for maintaining the integrity of the bank's systems and protecting sensitive data from cyber threats.

Secondly, studying the causes of employees' unawareness is vital for ensuring compliance with regulatory requirements. Financial institutions are subject to strict data protection and information security regulations, and addressing gaps in employees' knowledge and training is essential for meeting industry standards. By conducting thorough research into the factors contributing to employees' lack of awareness, banks can develop comprehensive training programs that align with regulatory expectations and help employees adhere to best practices in information security. This not only reduces the risk of non-compliance but also enhances the overall security posture of the institution.

Thirdly, understanding the causes of employees' unawareness of information security in banks can also help improve overall organizational culture and communication. By identifying factors such as lack of training, inadequate communication channels, or unclear policies, banks can address these issues to foster a culture of security awareness among employees. Clear communication of security policies, regular training sessions, and ongoing reinforcement of best practices can help create a security-conscious environment where employees understand the importance of safeguarding sensitive information.

Additionally, studying the causes of employees' unawareness can lead to the development of targeted awareness campaigns and initiatives that are tailored to address specific gaps in knowledge or behavior. By customizing training programs and communication strategies based on the identified root causes, banks can effectively engage employees and increase their understanding of security risks and protocols. This personalized approach can result in higher levels of awareness and compliance among staff members, ultimately strengthening the overall security posture of the bank.

In conclusion, studying the causes of employees' unawareness of information security in banks is essential for risk mitigation, regulatory compliance, organizational culture improvement, and targeted awareness initiatives. By identifying and addressing the root causes of employees' lack of awareness, banks can enhance their security

posture, protect sensitive data, and promote a culture of security awareness among staff members. This proactive approach is crucial for maintaining trust with customers, meeting regulatory requirements, and safeguarding the institution against cyber threats.

1.7 Scope of the Study

The scope of the research focus was on finding factors that lead to a lack of awareness about information system security in the case of Nib Bank at the branch level in Addis Ababa only.

The study was focused on examining, investigating, and understanding the factors that cause the unawareness of bank employees. The research takes awareness as the dependent variable while taking knowledge training, attitude, and perception as independent variables. It involved collecting data from employees who work at the branch level.

1.8 limitations of the study

The study on employees' unawareness of information security in banks encountered some limitations. Firstly, the reliance on self-reported data from employees about their knowledge, attitudes, and perceptions can introduce bias, as individuals may not always provide accurate information about their behaviors or beliefs. Additionally, the study's limited focus on analyzing the impact of specific training programs offered by the bank may overlook other sources of learning or external factors that contribute to information security awareness. A more comprehensive approach that considers informal learning and external influences could provide a more holistic understanding of employees' awareness levels.

Lastly, the study's timeframe for data collection may be constrained, limiting its ability to capture long-term trends in information security awareness or assess the effectiveness of ongoing training efforts. Information security awareness is a dynamic process that evolves over time, and a single snapshot may not fully reflect the changing nature of employee awareness within the bank.

1.9 Organization of the Study

This research is presented in a well-structured format consisting of five chapters. Chapter 1, titled "Introduction," lays the foundation for the entire study. It provides essential background information on the chosen field of research. This chapter also clearly defines the research problem being investigated, the

objectives the study aims to achieve, and any hypotheses it seeks to test. The significance of the research, the scope it covers, and any limitations it may have are also addressed in the first chapter.

Chapter 2, the "Literature Review," delves into existing knowledge relevant to the research topic.

Chapter 3, titled "Methodology," details the specific research methods employed in the study. This chapter sheds light on the research design, the chosen approach, and the sample selection process. The sources and methods of data collection, along with the data collection procedures and the methods used for data analysis, are all meticulously explained in this section.

Chapter 4, "Results and Discussion," presents the findings of the study. This chapter utilizes data analysis to reveal the research outcomes and interpret their meaning, providing a clear picture of what the study discovered.

Finally, Chapter 5, titled "Conclusion," summarizes the key findings of the research. It presents the conclusions drawn from the analysis and offers recommendations based on the overall outcomes of the study. This chapter effectively ties together the various elements of the research and provides a clear understanding of the research contribution.

Chapter two

Literature review

2.1 Overview

This section presents a review of related research on information security system breaches, awareness, threats, and information security system breaches in banks, as well as other related studies on information security system breaches.

2.3 Information Security System

Information security systems refer to a collection of policies, procedures, and technologies that are implemented to ensure the confidentiality, integrity, and availability of information. This system includes the recognition of potential threats to information assets, implementing controls to reduce those risks, and addressing security incidents through surveillance and response. Information security refers to the act of protecting information from unauthorized access, disclosure, interruption, interference, modification, or destruction. It strives to maintain the confidentiality, integrity, and practical availability of information through several risk management processes, such as providing assurances that data is not compromised (Michael, 2018).

The history of information security can be traced back to the days when the first computer systems were developed. Just at that moment, basic security measures included the physical protection of computer rooms and controlling access to keypunch machines. However, as computer systems proliferated and gained connectivity, the demand for more intricate security solutions increased. The emphasis changed to access control and authentication in the mid-1970s, where password systems appeared alongside encryption technologies developed throughout the late 20th century. Since the 21st century, information technology has brought new issues such as protection from hacking and viruses, along with other cyber-related acts of threat. This has resulted in the creation of new technologies and standards for information security, including firewalls, intrusion detection systems, and the ISO/IEC 27001 standard about the management's control over information safety. Information security remains the key issue for organizations of all sizes and types nowadays since cyber-attacks are becoming more advanced. Modern information security needs a three-dimensional approach and comprises technical controls, policy and procedure training, and awareness programs to achieve the underlying objective of monitoring and testing.

Information security is based on several layers of protection. These layers are built to offer comprehensive protection against possible threats and weaknesses. The last layer is security awareness and training, which ensures the sensitization of employees to the best practices, policies, and procedures associated with information security to reduce human error or insider threats. Security awareness programs may involve training, workshops, or online classes in which employees learn to identify threats and respond adequately (Rebekah and Robert, 2021).

2.4 Information Security System Threats

Dangers or adverse situations that may cause injury to a person, group, or system are referred to as threats. Cyber-threats entail malware, hacking attacks, data breaches, or any other activity posing a threat to computer security and integrity. In a broader perspective, threats can also be defined as possible risks or challenges that might negatively affect the safety of an individual or entity (Michael, 2018). Threats may be both human and non-human; however, the main threat to information security is a user of an information system unable to observe the necessary level of awareness in line with information policies (Siponen et al. 2014).

2.5 Information Security System Breach Awareness

The idea of awareness is the capacity to perceive, understand, and be aware of occurrences (Anthonia, 2020). According to another definition, it is the condition in which a subject is aware of information when it is immediately applicable to a variety of behavioral actions (Chalmers, 1997). According to Hussain et al. (2009), the idea is frequently used interchangeably with consciousness and is also thought to constitute awareness itself.

Awareness can be measured through various methods. There's no one-size-fits-all solution to measuring awareness. The key is to adopt a flexible and well-planned approach that aligns with the study's specific goals and resources. Usually, awareness is measured through employee’s knowledge, attitudes, perceptions, and training toward employee information security breaches (Schooll, 20).

Here are some ways to consider factors that affect awareness.

Knowledge

Awareness is based on knowledge. We do not comprehend how we can interpret the information from our sensory organs. Knowledge enables us to see patterns, draw inferences from them, and judge an outcome. This, on its own, makes us more aware of the activities that take place within our settlements (Pual, 2015).

Attitude

Our attitude towards something can also create our perception of it. A positive attitude allows us to observe closely and notice. However, when we have a negative attitude towards something, we tend to avoid paying attention to it and consciously ignore it (Richard, 1934).

Training

Training may also be used to increase awareness. Thus, training helps we understand that we can develop our senses and increase our attention spans by pointing out strategies and patterns. Thus, this may help us perceive better what goes around us (Ponnurangam, 2007).

For example, if you are trained on how to determine suspicious behavior and conduct activities, your chances of being aware of them when they happen increase. This is because you can recognize it based on the training that has equipped you with such skills and knowledge.

Perception

Perception is the act of interpreting sensory impressions. In other words, knowledge, attitudes, and expectations may play a significant role in perception (Icek, 2011).

Thus, awareness is influenced by knowledge, perception, attitude, and training, among many others. This information, therefore, allows us to take action that would increase our awareness and enable informed decisions regarding the quality of their lives.

According to Siponen (2000), information security system breach awareness is referred to as “a state where users in an organization are aware of their security mission," but a more extensive definition is also being used. Bulgurcu et al. (2010) define information security system breach awareness as an employee's knowledge and understanding of the requirements prescribed in the organization's data breach awareness policy and the aims of those requirements.

An activity that takes place within the organization's network and frequently leads to access to illegal data is known as an information systems security breach. (Angest et al., 2017) Such a breach might result in data loss, deletion of important information, alteration of stored data, and even theft of such data (Zafar et al., 2016).

Information security breach awareness covers a general understanding of an organization's security objectives and policies. Security awareness is one of the most recognized factors by researchers for improving information security practices (Siponen et al., 2014). Several concerns arise about data breach awareness. A survey conducted by the Ponemon Institute in 2023 shows that only about half of employees say they are extremely conscious of a potential data breach. According to IBM's 2021 report, the cost of information security breaches reached $4.35 million on average. This is worrying because employees provide the first line of defense for data breaches. Another study, which was published in the journal Information & Management 2021, concluded that there is a positive relationship between employee data breach awareness and organizational security posture. This shows that organizations investing in data breach awareness training are able to protect themselves from a data breach.

The importance of security awareness in improving information security procedures is well acknowledged by researchers (Siponen et al., 2014). Concern over awareness of data breaches is on the rise. Ponemon Institute, in its 2023 report, has asserted that only half of the employees are extremely aware of the possibility of a data breach. Secondly, the cost of an information security breach averaged approximately $4.35 million in 2022, a record-high figure according to IBM's Cost of a Data Breach Report for that year. Given that workers are frequently the first to detect and stop data breaches, this is alarming. In 2021, IBM revealed that as many as 59% of employees had already clicked on a phishing link in the last year. To ensure that their information is secure, employees must be familiar with the security standards of their organization and how they can adhere to them. This suggests that employees are not aware of data breaches and the risks; they are not always taking the necessary steps to protect themselves and the organizations they work for. Data breach awareness could be raised by giving insights about the breach and the threats and control mechanisms by training employees (Singh et al., 2014).

This means that if businesses invest in data breach awareness training, they have a better chance of protecting themselves from such threats. The organization should teach its employees about data breaches and why it's important. Employees should also know their roles and responsibilities for keeping information safe. They should report any security problems to their manager. It is also important that employees be aware of how much they can and cannot utilize the organization. However, if they violate the rules, they might be disciplined or punished (Singh et al. 2014). According to Alfawaz et al. (2010), four different employees' awareness arises from their understanding of information security breaches and security risks, and appropriate mitigating actions, behaviors, and knowledge-action states are depicted below:

Not Knowing, Not Doing: Employees are not aware of information security breaches and the organization's policies and rules regarding their role and consequently do not comply with them.

Not Knowing-Doing: Employees are not aware of information systems security rules but are behaving securely, usually due to organizational norms and culture that influence their awareness.

Knowing and Not Doing: Employees know the rules defined in the information security breach and the policy about information security breaches but are not following them consciously or unconsciously.

Knowing-Doing: Employees know the policy rules defined in the information security breach policy and are following them.

2.6 Information System Security Breach in Banks

Financial institutions, particularly banks, are most vulnerable to data breaches on account of the vital financial information they hold. Information security breaches can be not only rather disturbing for banks but also costly in terms of money and reputation. If financial impact is breached, then there are several financial losses banks incur, which can be direct costs that have to be investigated to remediate the breach, for example, legal fees, forensic analysis, and credit monitoring, and affected customers. Indirect costs include lost companies, damaged reputations, and frustrated customers. Reputational banks can also be adversely affected by information system breaches to a great extent. With a loss of trust, clients may be lost due to data breaches at banks. This results in customer deposits and revenue losses. Furthermore, information security violations can harm a bank’s reputation. Negative media attention can make it difficult for a bank to grow its client base and maintain the old ones (Van & Von, 2013).

When bank employees use their computers to access banking websites, there's a risk that someone could steal information. This can happen because some websites have weaknesses that let bad guys put harmful code or commands into the site. This could give them access to the bank's databases and sensitive information. Other flaws may stem from inadequate banking security policies and poor usability practices (Jassal & Sehgal, 2013).

Vrincianu & Pop (2010) identified the primary threats or attacks to the security of banking platforms. The first one is DoS attacks, which aim to overload a system with traffic so that legitimate users are unable to access it. Secondly, illegitimate use refers to unauthorized access to banking accounts to steal money or conduct fraudulent transactions. Thirdly, disclosure of information involves the unauthorized access and sharing of sensitive customer data, such as account numbers, passwords, and personal information. And finally,

repudiation occurs when a user attempts to deny a transaction they have made, claiming that it was unauthorized or fraudulent.

Peotta et al. (2011) proposed a classification of common attacks against online banking systems based on three major categories. The first one is legitimate access, which is when access attacks exploit vulnerabilities in banking systems to gain unauthorized access to user accounts without the knowledge or consent of the account holder. The second is device control attacks, which target to commandeer a user's device, such as their smartphone or computer, and the third is credential theft, which involves stealing a user's credentials and log-in credential information. Even though there are several threats, the most critical threat is an employee who lacks the knowledge and skill to breach them and how to control them (Jang & Nepal, 2014).

2.7 Related Studies in Ethiopia

One of the related studies conducted by Abiy et al. (2019) revealed that the level of information security awareness in the Ethiopian banking sector is inadequate. Girma (2020) also found that factors such as information systems security policy, organizational culture, and employee awareness have an impact on the current practices of information systems security in banks. Insufficient employee training and awareness of information systems security policies were identified as major issues in securing data and information. To address this gap, banks should prioritize employee education and awareness to improve their information system security practices. Woretaw and Lessa (2012) concluded that the level of awareness among employees in the Ethiopian banking sector is inadequate. Similarly, a study by Milkyas & Lemma (2019) conducted a case study using a quantitative research approach and found that Enat Bank employees had an unsatisfactory level of information security awareness. The researchers proposed a program to assist the bank in creating information security awareness and good practices among its employees to strengthen its security posture and mitigate vulnerabilities to computer attacks. Recommendations were also provided for short- and long-term improvements in employees' information security awareness. Despite these studies, there still exists a gap in the banking industry regarding employee awareness and the underlying reasons for insufficient awareness.

2.8 Conceptual framework

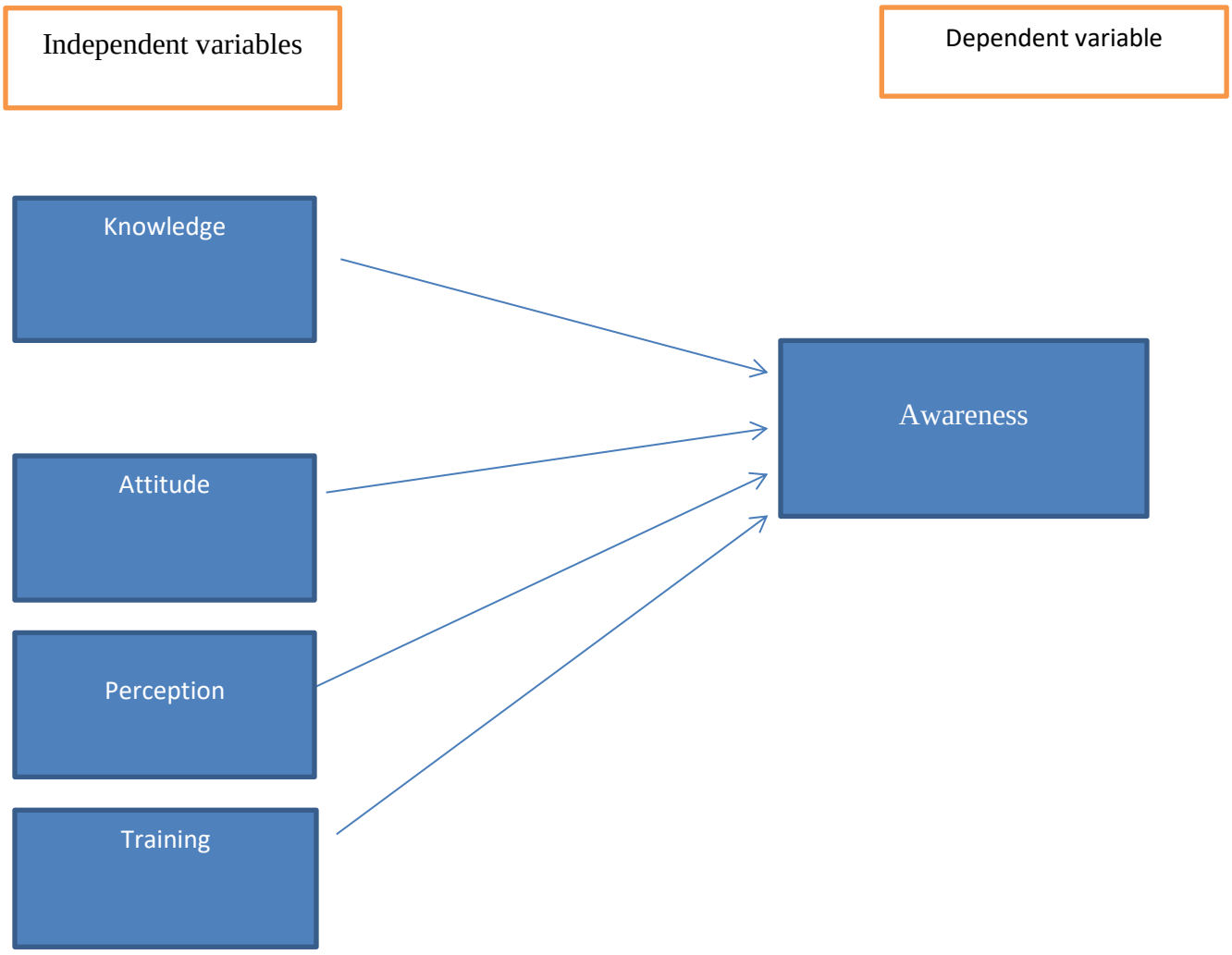
The Knowledge, Attitude, Perception and training framework is a conceptual model used to understand how employees develop awareness about information system security.

Knowledge: This refers to an employee's understanding of information security concepts, policies, and best practices. Strong knowledge equips employees to identify potential threats and vulnerabilities.

Perception: This encompasses how employees interpret and view security risks. Even with good knowledge, a negative perception (e.g., security procedures are too cumbersome) can hinder awareness and lead to risky behavior.

Attitude: This reflects an employee's feelings and beliefs towards information security. Positive attitudes (e.g., understanding the importance of data protection) are crucial for translating knowledge into responsible behavior.

Training: This refers to any interventions designed to improve security knowledge, address misperceptions, and cultivate positive security attitudes.


Independent variables
Dependent variable
Knowledge
Attitude
Perception
Training
Awareness

3. Chapter three

Methodology

3.1. Research Approach

The study is carried out according to several protocols, procedures, and criteria. However, using quantitative methods is the most appropriate way to do this research. A set number of respondents, a list of questions, and planned response options were all part of the quantitative approach. The researcher utilized a quantitative research approach to analyze and process data from large samples using reliable and consistent procedures for quantitative data analysis.

3.2 Research Design

The research design used is a cross-sectional design. This design is appropriate as it allows for the collection of data from a sample at a specific point in time. The purpose of explanatory Causal research can be carried out to evaluate the effects of particular modifications on standard practices, different procedures, etc. This implies that the awareness of employees will be affected by their knowledge of security threats, attitude towards security procedures, perception of security risks, and participation in security training. determining if and to what degree they have a positive or negative relationship.

3.3 Population and Sample

The population for this study was NIB bank employees. Employees, those with computer access who regularly interacted with computer systems were considered more likely to access and process sensitive information. This included customer data, financial records, and internal bank documents, making them prime targets for cyber-attacks. Employees engaged in online activities like sending and receiving emails, accessing web applications, and downloading files could have introduced security vulnerabilities if proper protocols were not followed. They also managed digital assets like usernames, passwords, and access credentials associated with computer systems, requiring careful management to prevent unauthorized access.

The sampling technique used in this study was proportional sampling. Nib Bank employees utilized a sample of 400 bank employees drawn from a total population of 8,000. This sample size represented 5% of the total population and was used to study and analyze the various factors which were the desired sample. Therefore the researcher took two groups the front line and the back office employees.

Sample size for back front line employees	Sample size for back office employees
Proportion of front line: 62.7%	Proportion of back office employees: 37.3%
Sample size for front line =Proportion of front line * Total desired sample size	Sample size for back office employees = Proportion of back office employees * Total desired sample size
Sample size for front line = 0.627 * 404	Sample size for back office employees = 0.373 * 4000
Sample size for front line = 0.627 * 400	Sample size for back office employees = 0.373 * 400
Sample size for front line = 250.8 (rounded to 251)	Sample size for back office employees = 149.2 (rounded to 149)

Therefore, the researcher initially enrolled 400 employees who were closest to the problem under study. However, to increase the study's reliability, the number of respondents was increased beyond the initial sample size which was 455.

3.4 Data Sources and Types

The primary data for this study were obtained through a researcher-distributed questionnaire administered to various bank employees. Secondary data were obtained by reviewing previous research studies.

3.5 Data Collection Procedures

A survey questionnaire was employed to gather data from bank employees for this study. This structured questionnaire was designed to delve into four key areas: employee knowledge of security threats, their attitudes toward security procedures, their perceptions of security risks, and their participation in security training. Demographic information was also collected from the participants to provide context for the analysis. The questionnaires were distributed in person to the bank employees, ensuring a high response rate and facilitating clarification of any questions that might arise. The study preprocessed the data after collection, converting it to an Excel format and then importing it into SPSS. This allowed for the identification of outliers and missing data which was 23 data’s out of 455.

3.6 Validity and reliability

3.6.1 Validity Test

A quantitative researcher should take validity and reliability into account when evaluating the study's quality, designing the investigation, and interpreting the findings, according to Patton (2001). Research philosophies and techniques are typically connected (Saunders et al., 2007). Therefore, the research goal and methodologies were closely examined to guarantee the validity of this study. To maintain the validity of the research, questions were created based on the theory of planned behavior and literature already in existence that was pertinent to the study's issue (Ajzen,2001). The study's reliability is deemed high due to the major source of information obtained through questioning techniques as well as the application of pertinent theories. The respondents that were chosen are bank employees. To enhance comprehension and validate the study's dependability, a structured approach is employed throughout the research procedure.

3.6.2Reliability

The regularity and dependability of measurement devices are referred to as reliability. To determine if it is appropriate to depend on the respondents' responses, one of the internal consistency techniques for reliability assessment—the corn batch alpha coefficient—was used. For a coefficient to be deemed dependable, it must fall between 0 and 1. The item's internal consistency is improved because the result is getting closer to 1, indicating that all of the items measure the same thing—that is, the overall ethical standard and service quality. As a result, the coefficient of this research has lied close to 1.

3.7 Data Analysis

The statistical procedures utilized in this study—multiple regression analysis, correlation analysis, and descriptive analysis—were all performed using the Statistical Package for Social Science (SPSS) software to analyze and present the data.

Descriptive Analysis

To provide a simplified view of the data, tables, frequency distributions, and percentages were used to display the descriptive statistical results. Summary statistics, which are used to calculate the means and standard deviations for each variable in the study, were used to do this. In data analysis, descriptive statistics are

employed to examine the characteristics and distribution of the collected data. Inferential statistics like regression and correlation analysis are used to examine the connection between this awareness and knowledge of security threats, attitude towards security procedures, perception of security risks, and participation in security training among employees.

Correlation Analysis

The degree of correspondence between variables is known as correlation. This suggests that the relationship is reciprocal or mutual, but according to Roby (2022), "we did not include any proposition that one thing is the cause and the other the effect in our concept of correlation." This definition guides the use of correlation analysis in this study, which looks at the strength of the relationship between the variables under investigation. This research examines the associations between the employee's unawareness and their knowledge of security threats, attitude towards security procedures, perception of security risks, and participation in security training multiple regression analysis was used to investigate the effect of knowledge perception, attitude, and training at Nib International Bank.

Regression functions

The dependent variable in this study is awareness, and the independent variables are knowledge, perception, attitude, and training. These two sets of variables serve as the foundation of the multiple regression equation. Regression equations are primarily used in studies to help researchers better understand, predict, describe, and manage the variables that are being studied.

3.8 Ethical Considerations

The study required addressing ethical concerns surrounding informed consent, participant data confidentiality, and potential harm to participants.

Chapter four

Data analysis and discussion of results

In this chapter as discussed earlier in chapter one data were collected, based on the research objectives, are properly presented, analyzed and discussed. More than four fifty questionnaires were distributed and four hundred thirty three were collected from employees in different NIB branches. This study intends to look into why bank employees are unaware of information system security.

4.1. Descriptive statistics

In these regard respondents were asked to indicate the degree of service quality using a five point likert scale where 5 represents Strongly agreed, 4 represent agree, 3 represent Indifferent, 2 represent disagreed and 1 represent Strongly disagreed.

Table 1 descriptive statistics for knowledge

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Knowledge [The CIA triad (confidentiality, integrity, and availability) for information security is a complex topic that may require further clarification for me?]	434	2	5	3.96	.715
Knowledge [Creating and managing strong passwords according to bank guidelines can be a challenging process. I would appreciate additional resources or support?]	434	1	5	3.75	1.062
Knowledge [Identifying red flags in phishing attempts can be tricky, More examples and practice scenarios would be helpful?]	434	1	5	3.68	.932
Knowledge [The bank's policies on data encryption, sharing, and disposal can be quite detailed. A quick reference guide or refresher training would be beneficial?]	434	1	5	3.93	.864
Knowledge [Reporting suspicious activity can be a sensitive situation. Having clear guidelines and channels for reporting would make me more comfortable?]	434	1	5	3.85	1.053
Valid N (listwise)	434				

Source: Primary data, 2024.

The data appears to be measuring the bank employees' training and understanding of various information security-related topics. Here's the interpretation of the key findings the results are indicating that respondents have a lack understanding of the CIA triad and its components. Here is a summary of the findings:

Interpreting the CIA Triad

Respondents rated their understanding of the CIA triad as moderately low, with a mean score of 3.96 out of 5, indicating a lack of the concept.

Managing Strong Passwords

Participants found creating and managing strong passwords challenging, suggesting a need for additional resources or support, with a mean score of 3.75 out of 5.

Identifying Phishing Red Flags

Recognizing red flags in phishing attempts was perceived as tricky, indicating a desire for more examples and practice scenarios, with a mean score of 3.68 out of 5.

Bank Policies on Data Security

Understanding bank policies on data encryption, sharing, and disposal was rated positively, with a mean score of 3.93 out of 5, suggesting a need for quick reference guides or refresher training.

Reporting Suspicious Activity

Participants expressed a need for clear guidelines and channels for reporting suspicious activity, with a mean score of 3.85 out of 5, highlighting the importance of feeling comfortable when reporting such incidents.

Overall, the data reflects a lack in knowledge of awareness of cyber-security concepts like the CIA triad, and also indicates areas where individuals may require further support or resources to enhance their cyber-security practices, especially in managing passwords, identifying phishing attempts, and reporting suspicious activities.

Table 2 Descriptive statistics for perception

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Perception [I believe that I am less likely to encounter a phishing attempt in my work emai?]	434	2	5	4.04	.643
Perception [The bank's information security policies are clear and easy to understand?]	434	2	5	3.68	1.099
Perception [I am responsile responsible for maintaining good information security practices?]	434	2	5	3.56	.916
Perception [Following information security procedures hinders my ability to get my job done efficiently?]	434	1	5	3.94	.893
Perception [The bank's current security measures are adequate to protect against cyber-attacks?]	434	1	5	3.90	1.018
Valid N (listwise)	434				

Source: Primary data, 2024

The data appears to be measuring the bank employees' perception and understanding of various information security-related topics. Here's the interpretation of the key findings the survey assessed their views on various aspects of security, including their likelihood of encountering phishing attempts, the clarity of bank policies, their sense of responsibility for maintaining good security practices, the impact of security procedures on their work efficiency, and the adequacy of the bank's security measures against cyber-attacks. The results indicate that the employees have a generally negative perception of these aspects of information systems security.

Perception of Phishing Attempts

The majority of employees (4.04 out of 5) believe they are less likely to encounter phishing attempts in their work email. This suggests that they may be overconfident in their ability to detect phishing attempts. Clarity of Bank Policies: The employees have a relatively low perception (3.68 out of 5) of the bank's information security

policies being clear and easy to understand. This indicates that there may be a need for better communication and clarification of security policies.

Responsibility for Security Practice

The employees have a moderate perception (3.56 out of 5) of being responsible for maintaining good information security practices. This suggests that they may not fully understand their role in maintaining security or may not feel empowered to take responsibility.

Impact of Security Procedures

The majority of employees (3.94 out of 5) believe that following information security procedures hinders their ability to get their job done efficiently. This indicates that the security procedures may be overly restrictive or burdensome, leading to frustration among employees.

Adequacy of Security Measures

The employees have a moderate perception (3.90 out of 5) of the bank's current security measures being adequate to protect against cyber-attacks. This suggests that there may be concerns about the effectiveness of the security measures in place.

Conclusion

The data suggests that bank employees have a generally negative perception of information systems security. They may be overconfident in their ability to detect phishing attempts, feel that security policies are unclear, and believe that security procedures hinder their work efficiency. Additionally, there may be concerns about the adequacy of the bank's security measures against cyber-attacks. These findings highlight the need for improved communication, clearer policies, and more effective security measures to enhance the employees' perception of information systems security.

Table 3 Descriptive statistics for attitude

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Attitude [i believe their are critical priority than Information security for the bank's success?]	434	2	5	4.00	.681
Attitude [I do find the bank's information security procedures to be complicated?]	434	1	5	3.74	1.090
Attitude [I am confident in the bank's ability to protect sensitive information from security threats?]	434	2	5	3.66	.923
Attitude [I feel less comfortable reporting security concerns or violations without fear of reprisal?]	434	1	5	3.92	.899
Attitude [I believe that I am less likely to encounter a phishing attempt in my work email?]	434	1	5	3.89	1.009
Valid N (listwise)	434				

e

Source: Primary data, 2024

The data appears to be measuring the bank employees' attitude and understanding of various information security-related topics. Here's the interpretation of the key findings

Priority of Information Security

The majority of employees (4.00 out of 5) believe that there are critical priorities other than information security for the bank's success. This suggests that they may not consider information security as a top priority.

Complexity of Security Procedures

The employees have a relatively low perception (3.74 out of 5) of the bank's information security procedures being complicated. This indicates that they may find the procedures overly complex or difficult to follow.

Confidence in Security Measures

The employees have a moderate perception (3.66 out of 5) of being confident in the bank's ability to protect sensitive information from security threats. This suggests that they may have some doubts about the effectiveness of the bank's security measures.

Reporting Security Concerns

The majority of employees (3.92 out of 5) feel less comfortable reporting security concerns or violations without fear of reprisal. This indicates that there may be a lack of trust or fear of retaliation among employees when reporting security issues.

Phishing Attempts

The employees have a moderate perception (3.89 out of 5) of being less likely to encounter a phishing attempt in their work email. This suggests that they may not be confident in their ability to detect phishing attempts. The data suggests that bank employees have a generally negative attitude towards information systems security. They may not consider information security as a top priority, find security procedures overly complex, have doubts about the effectiveness of security measures, feel uncomfortable reporting security concerns, and lack confidence in detecting phishing attempts. These findings highlight the need for improved communication, clearer policies, and more effective security measures to enhance the employees' attitude towards information systems security.

Table 4 Descriptive statistics for training

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Training [The information security awareness training content was confusing at times and required me to refer to other resources for clarification?]	434	1	5	4.00	.732
Training [The information security awareness training focused on general security threats, but it lacked specific examplesrelevant to the types of attacks I might encounter in my role?]	434	1	5	3.69	1.080
Training [Some of the information security awareness training contents were outdated and were not much of a use in the current technology system?]	434	2	5	3.67	.891
Training [The information security awareness training was presented in a lecture format, which I found rather passive and didn't encourage much active participation?]	434	1	5	3.94	.890
Training [The information security awareness training covered a broad range of topics, but it didn't provide enough depth on any specific security threats or procedures?]	434	1	5	3.90	.955
Valid N (listwise)	434				

Source: Primary data, 2024

The data appears to be measuring the bank employees' training and understanding of various information security-related topics. Here's the interpretation of the key findings:

Clarity of Training Content

Respondents found the training content confusing at times, with a mean score of 4.00 out of 5, indicating a need for clearer and more concise presentation of information.

Relevance of Examples

Participants felt that the training lacked specific examples relevant to the types of attacks they might encounter in their roles, with a mean score of 3.69 out of 5, suggesting a need for more targeted and practical examples.

Currency of Information

Some respondents found the training content outdated and not very useful in the current technology landscape, with a mean score of 3.67 out of 5, highlighting the importance of regularly updating training materials.

Training Format

The lecture format of the training was perceived as passive and not encouraging active participation, with a mean score of 3.94 out of 5, indicating a need for more interactive and engaging training methods.

Depth of Coverage: While the training covered a broad range of topics, it did not provide enough depth on specific security threats or procedures, with a mean score of 3.90 out of 5, suggesting a need for more focused and in-depth coverage of critical security areas.

Overall, the data reflects a general dissatisfaction with the quality and effectiveness of the information security awareness training programs. The findings suggest that organizations should focus on improving the clarity, relevance, currency, format, and depth of their training content to better prepare employees for the evolving security landscape.

Table 5 Descriptive statistics for awareness

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Awareness [Their is lack of awareness on how serious threats are cyber-attacks to the bank's security?]	434	3	5	4.06	.616
Awareness [Their is difficullty in my ability to identify the signs of a malware infection on a work computer?]	434	2	5	3.70	1.093
Awareness [The bank encourages employees to report any suspicious activity related to information security. I am comfortable discussing such concerns with supervisor or the IT?]	434	2	5	3.62	.915
Awareness [Following information security procedures can sometimes feel time-consuming?]	434	1	5	3.96	.860
Awareness [Data breaches can occur when sensitive information falls into the wrong hands?]	434	1	5	3.89	1.023
Valid N (listwise)	434				

Source: Primary data, 2024

The data appears to be measuring the bank employees' awareness and understanding of various information security-related topics. Here's my interpretation of the key findings:

Awareness of Cyber Attack Threats

The employees agreed that there is not enough awareness (4.06 out of 5) that cyber-attacks pose serious threats to the bank's security. This suggests that the employees lacks to understand the gravity of the cyber security risks facing the organization.

Ability to Identify Malware Infections

The employees have a low level of (3.70 out of 5) regarding their ability to identify the signs of a malware infection on a work computer. This indicates that there may be a need for more training or resources to help employees better recognize and respond to malware threats.

Comfort in Reporting Suspicious Activity

The employees have a relatively lower level of comfort (3.62 out of 5) regarding the bank's encouragement to report suspicious activity and their comfort in discussing such concerns with supervisors or the IT department.

This suggests that the bank may need to improve its communication and create a more supportive environment for employees to report security-related issues.

Perception of Security Procedures

The employees have negative perception (3.96 out of 5) that following information security procedures can sometimes feel time-consuming. This indicates that the employees may perceive the security procedures as burdensome, which could impact their compliance and engagement with security practices.

Awareness of Data Breaches

The employees have a moderate level of (3.89 out of 5) that data breaches can occur when sensitive information falls into the wrong hands. This suggests that the employees understand the potential consequences of data breaches, but there may be room for improvement in their overall security awareness.

Overall, the data suggests that the bank's employees have a generally lack understanding of the cybersecurity threats and risks facing the organization. Therefore, there are some areas, such as malware identification, reporting of suspicious activity, and the perceived burden of security procedures, where additional training or communication may be beneficial to enhance the employees' security awareness and engagement.

4.3 Correlation Analysis

Correlation is the degree of correspondence between variables. Based on this definition, this study employs correlation analysis to investigate the strength of the relationship between the studied variables. Coefficient of correlation of the variables lies between -1 and +1. Accordingly, -1 means perfect negative correlation, increase from -1 to 0 negative correlation decrease, 0 implies there is no correlation, increase from 0 to +1 positive correlation increase and +1 means perfect positive correlation

Table 6 correlation analysis

Correlations

		AW_MEAN	P_MEAN	A_MEAN	T_MEAN	K_MEAN
AW_MEAN	Pearson Correlation	1	.733**	.746**	.595**	.758**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	434	434	434	434	434
P_MEAN	Pearson Correlation	.733**	1	.689**	.600**	.615**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	434	434	434	434	434
A_MEAN	Pearson Correlation	.746**	.689**	1	.569**	.742**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	434	434	434	434	434
T_MEAN	Pearson Correlation	.595**	.600**	.569**	1	.588**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	434	434	434	434	434
K_MEAN	Pearson Correlation	.758**	.615**	.742**	.588**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	434	434	434	434	434

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Primary data, 2024

Awareness (AW_MEAN) has a strong positive correlation with Perception ($r=0.733$, $p<0.01$), Attitude ($r=0.746$, $p<0.01$) and Knowledge ($r=0.758$, $p<0.01$). This suggests higher awareness is associated with more positive perceptions, attitudes and knowledge regarding information security. Awareness also moderately correlates with Training ($r=0.595$, $p<0.01$).

In summary, the factors are positively associated. Improving one, like training, could enhance employee awareness, perceptions, attitudes and knowledge regarding information security. The strong correlations suggest these aspects are closely intertwined.

4.4 Regression analysis

The study further conducted inferential analysis which involved a correlation analysis and a multiple regression analysis. The inferential analysis was intended to establish the relationship between the independent variables and the dependent variable of the study.

Table 5 Model Summary

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.843[a]	.711	.708	.40750	1.969

a. Predictors: (Constant), K_MEAN, T_MEAN, P_MEAN, A_MEAN

b. Dependent Variable: AW_MEAN

Source: Primary data, 2024

The R_0.843 has represented a moderately strong positive correlation between the predicted and actual values of awareness (AW_Mean), with R-squared: 0.711 - This value indicates that 71.1% of the variance in awareness can be explained by the independent variables (knowledge, attitude, perception and training) in the model. In addition the Adjusted R-squared (0.708) value adjusts for the number of independent variables, providing a more accurate estimate of the model's explanatory power. It's slightly lower than R-squared, suggesting that the model's explanatory power might be slightly inflated due to its complexity. Furthermore Std. Error of the estimate (0.40750) value has represented the standard deviation of the residuals (difference between predicted and actual values). A lower value indicates a better fit of the model to the data. The Durbin-Watson (1.969) has suggested no significant autocorrelation in the residuals. The model shows a positive relationship between the values (knowledge, attitude, perception and training) and awareness. While 71.1% of the variance is explained, there might be other factors influencing awareness that are not captured by this model. The adjusted R-squared suggests a reasonable fit for the model's complexity. However, 28.9 of the variance is explained by other there might be other factors influencing awareness that are not captured by this model.

Table 6 ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	175.082	4	43.770	263.582	.000[b]
	Residual	71.240	429	.166		
	Total	246.321	433			

a. Dependent Variable: AW_MEAN

b. Predictors: (Constant), K_MEAN, T_MEAN, P_MEAN, A_MEAN

Source: Primary data, 2024

The model provides an explanation for 175.082 units of the total variance, which accounts for approximately 71.1% of the variance based on the R-squared value. Although the R-squared value is not explicitly shown in the table, it can be obtained from previous analyses. The high F-statistic of 263.582 and a significant p-value of 0.000 indicate that the independent variables - knowledge, attitude, perception, and training - significantly contribute to explaining the variance in awareness compared to simply using the mean.

Furthermore, the ANOVA table reveals that the dependent variable, awareness, and the four independent variables (knowledge, attitude, perception, and training) are statistically significantly correlated. This suggests that awareness is indeed impacted by at least one of these factors.

Table 7 Coefficient for awareness

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	.845	.095		8.925	.000	.659	1.032		
	P_MEAN	.296	.036	.321	8.340	.000	.226	.366	.454	2.201
	A_MEAN	.206	.040	.222	5.116	.000	.127	.285	.359	2.786
	T_MEAN	.056	.030	.065	1.871	.062	-.003	.114	.557	1.795
	K_MEAN	.327	.037	.358	8.743	.000	.253	.400	.403	2.484

a. Dependent Variable: AW_MEAN

Source: Primary data, 2024

The "Coefficients" table provides information about the regression coefficients and their statistical significance. Here's a detailed interpretation:

The analysis provides detailed information about the coefficients and their significance in the regression model. The constant term (0.845) represents the expected value of the dependent variable (AW_MEAN) when all predictors are zero. In this case, it signifies the baseline level of awareness when knowledge, attitude, perception, and training are all at their minimum values.

The coefficients for the predictors reveal the impact of each predictor on the awareness mean (AW_MEAN). The positive coefficient for P_MEAN ($B = 0.296$, $p < 0.001$) indicates that an increase in perception is associated with a significant positive effect on awareness. Similarly, A_MEAN has a significant positive effect on AW_MEAN ($B = 0.206$, $p < 0.001$), suggesting that higher levels of attitude are linked to increased awareness. K_MEAN also has a significant positive effect on AW_MEAN ($B = 0.327$, $p < 0.001$), indicating that higher knowledge levels are associated with higher awareness. On the other hand, T_MEAN has a marginally significant positive effect ($B = 0.056$, $p = 0.062$), suggesting that its impact on awareness is not statistically significant at the conventional 0.05 significance level.

The standardized coefficients further highlight the relative importance of each predictor. K_MEAN has the strongest effect on AW_MEAN, followed by P_MEAN, A_MEAN, and T_MEAN. This information provides insights into which factors have the most substantial influence on awareness in the context of this analysis.

Chapter five

Summary, Conclusion, And Recommendation

5.1 Summary of Findings

Firstly, the study revealed a significant knowledge gap. Employees lacked a fundamental understanding of common security threats like phishing emails and malware. This knowledge gap proves critical, as employees are unable to recognize these deceptive tactics. Imagine an employee receiving an email that appears to be from their bank, requesting login information. Without the knowledge to identify the significant signs of a phishing attempt, the employee becomes susceptible to clicking malicious links or exposing sensitive data, unknowingly compromising the bank's security.

Secondly, the study highlighted a negative perception and attitude of security procedures. Employees might view firewalls, password complexity requirements, and access restrictions as bothersome hurdles that slow down their work. This perception undermines the effectiveness of these very measures designed to protect the bank.

Finally, the study identified inadequacies in existing security training programs. These programs are outdated, leading to poor information retention. Alternatively, they might fail to comprehensively cover essential security concepts, leaving employees unprepared for the ever-evolving cyber threat landscape. This lack of effective training creates a blind spot, leaving employees unaware of the latest threats and best practices to defend themselves and the organization's data.

These three issues – knowledge gaps, negative perception, and inadequate training – combine to create a significant security risk. Employees become easy targets for attackers, potentially leading to data breaches, financial losses, and reputational damage for the bank.

5.2 Hypothesis Testing

Awareness is positively impacted by knowledge. Thus we can reject “Hypothesis 1: Knowledge does not significantly affect awareness”

Awareness is positively impacted by perception. Thus, we can reject “Hypothesis 2: Perception does not significantly affect awareness.”

Attitude Awareness is positively impacted by attitude. Thus we are able to reject “Hypothesis 3: Attitude does not significantly affect awareness.”

Training and awareness are slightly negatively correlated resulting less impact on awareness.

5.3 Conclusion

The study revealed a critical gap in employee information security awareness. The identified knowledge gaps, coupled with negative perceptions and attitudes towards security measures, create a significant vulnerability for organizations. Employees lacking basic knowledge about security threats, like phishing attempts, are unable to recognize them, leaving the bank data exposed. Furthermore, a negative perception of security procedures as bothersome or unnecessary hinders their effectiveness.

To address these issues, the bank needs a comprehensive strategy that tackles knowledge, perception, and attitude. Firstly, security awareness training programs should be designed to bridge the knowledge gap. Interactive and engaging training can foster a deeper understanding of information security best practices, making them relevant and memorable. Secondly, the training should address negative perceptions by highlighting the importance of security measures in protecting sensitive information and the organization's reputation. By framing security procedures as safeguards rather than obstacles, employee attitudes can shift towards a sense of shared responsibility.

Finally, fostering a culture of open communication is essential. The bank should encourage employees to report suspicious activity and discuss security incidents openly. This promotes ongoing learning and reinforces the importance of information security. By continuously reviewing and updating training programs and conducting phishing simulations, organizations can assess their effectiveness and identify areas for improvement. This proactive approach empowers employees to become the first line of defense against cyberattacks. Addressing knowledge gaps, and negative perceptions, and fostering positive security attitudes will lead to a more secure work environment for everyone, minimizing risks and safeguarding valuable information.

5.4 Recommendations

To address these critical issues and improve employee awareness of information security, the following recommendations are proposed:

To address the critical security gap identified in the study, a multi-pronged approach is recommended. First, to enhance information security awareness and mitigate the risk of data breaches, banks should implement a mandatory, pre-employment information security module for all employees. This comprehensive module should be regularly updated to reflect the evolving cyber threat landscape and equip new hires with the essential knowledge and skills to identify, prevent, and report security incidents. Enhanced security training is crucial. Training content should be comprehensive, covering various topics from common threats to secure browsing habits. Interactive elements like simulations and results can improve engagement and knowledge retention. Additionally, training should be tailored to different employee roles, with executives receiving an overview and technical staff getting in-depth training.

Secondly, promoting a positive security culture is essential. Regular communication campaigns using diverse channels like emails and posters can keep security awareness high. Strong leadership support is vital, with leaders actively promoting security, demonstrating good practices, and recognizing security-conscious employees.

Thirdly, reinforcing security policies is necessary. Clear, concise, and jargon-free policies outlining acceptable and unacceptable practices should be readily accessible to all employees. Regular reviews and updates are crucial to adapting to the evolving threat landscape.

Finally, measuring and improving training effectiveness is key. Pre- and post-training assessments, security attitude surveys, and simulated phishing attacks can be used to evaluate knowledge retention and identify areas for improvement. Based on this data, training content and delivery methods can be continuously refined to ensure a well-trained and security-conscious workforce. By implementing these recommendations, organizations can empower employees to become the first line of defense against cyber threats, significantly improving their overall information security posture.

Reference

Antony,s. (2009). " The impact of information security awareness training on information security behavior," Thesis.

Anthonia,P.(2020). Awareness and Purpose of Electronic Information Resources among Postgraduate Students of Library and Information Science in Born State

Abbate, J.(2000). Inventing the Internet, Cambridge, Mass.: The MIT Press.

Abiy W., et. al., (2019). Factors Hindering Full Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture. Twenty-fifth Americas Conference on Information Systems, Cancun.

Accenture, (2020). Cost of Cyber Crime Study: Financial Services.

Adane, K. (2020). The Current Status of Cyber Security in Ethiopia (2020) .

Anderson, C., and Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly, Vol. 34, No. 3, pp 613-643.

Alfawaz S, et al., (2010). Information Security Culture: A Behaviour Compliance Conceptual Framework. Conferences in Research and Practice in Information Technology Series 105:pp 47–55.

Albrechtsen, E., Hovden, J., & Kydland, T. (2017). Information security culture in banking. Computers & Security, 68, 45-61.

Angst, C. M. Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. MIS Quarterly, 41(3),pp. 893-916.

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

Bartlomiej,H. and Yu,A. (2016). "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," Inf. Syst. Manag., vol. 33,no. 1, pp. 2–16, Jan.

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), pp. 523–548.

Chalmers, David (1997). The Conscious Mind: In Search of a Fundamental Theory: Oxford University Press. pp. 225

Furnell, S., & Karweni, T. (2018). Security awareness and training: A review of human factors in information security. Computers & Security, 78, 398-410.

Girma,A. (2020) A Framework For Human Factors Influence On Information Systems Security At Commercial Banks In Ethiopia,

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S.A. (2017). "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach," MIS Quarterly (41:3), pp. 703-727.

Hussain, A., Alexander, I., Smith. L.,; Barros, A., Chrysler., Cutsuridis, V. (2009). Brain Inspired Cognitive Systems 2008 New York: Springer Science+Business Media. pp. 298

Icek,A.(2011)“The theory of planned behaviour: Reactions and reflections,” Psychol. Health, vol. 26, no. 9, pp. 1113–1127.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. Journal of Computer & System Sciences, 80(5), pp. 973-993.

Jassal, R. & Sehgal, R. (2013). Online Banking Security Flaws: A Study. International Journal of Advanced Research in Computer Science and Software Engineering, 3(8), 1016 – 1021.

Kim, E.B. (2014). Recommendations for Information Security Awareness Training for College Students. Information Management & Computer Security, Vol 22(1), pp.115-126.

Lee, B. (1999) Pragmatics of Community Organization. 3rd Edition, Common Act Press Canada, Ontario (Canada).

Metalidoua E, et.al., (2014). The Human Factor of Information Security: Unintentional Damage Perspective, Procedia-Social and Behavioral Sciences, pp.147.

Michael E. Whitman and Herbert J. Mattord Principles of Information Security, Sixth Edition pp. 60

Milkyas, B., Lemma,L.(2019) Building an Information Security Awareness Program for a Bank: Case from Ethiopia

Paul m. leonardi (2015) ambient awareness and knowledge acquisition: using social media to learn “who knows what” and “who knows whom”mis quarterly vol. 39 no. 4, pp. 747-762.

Peotta, L., et. al., (2011). A Formal Classification of Interest Banking Attacks and Vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT), 3(1), pp.186 – 197.

Pollock T., (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS), KSU Proceedings on Cyber security Education, Research and Practice, Kennesaw State University pp.30-69.

Ponnurangam,K. et al .,(2007) . “Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System,” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA, 2007, pp. 905– 914.

Rebekah, B. & Robert, M.(2021) SANS Cyber Threat Intelligence (CTI) Survey

Richard. T., (1934.) “Attitudes vs. Actions,” Soc. Forces, vol. 13, no. 2, pp. 230–237.

Roby, S. (2022). The Effect of Perceived Price and Service Quality

Singh, N, et al., (2014). Identifying Factors of Organizational Information Security Management. Journal of Enterprise Information Management, Vol 27(5) pp. 644-667.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. Information Management and Computer Security, 8(1), 31–41.

Siponen, M. T., et. al., (2014). Employees’ Adherence to Information Security Policies: An Exploratory Field Study. Information &Management, 51(2), 217-224.

Smith, Joel (2020), Zalta, Edward N. (ed.), "Self-Consciousness", The Stanford Encyclopedia of Philosophy (Summer 2020 ed.), Metaphysics Research Lab, Stanford University, retrieved 2023-pp.10-25

Scholl, M., Leiner, K. B., & Fuhrmann, F. (2017). Blind spot: Do you know the effectiveness of your Information security awareness-raising program? WMSCI 2017 - 21st World Multi-Conference on Systemics, Cybernetics and Informatics, Proceedings pp.361–366

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers and Security, pp. 124–133.

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

Vrincianu, M. & Popa, L. (2010). Considerations Regarding the Security and Protection of E- Banking Services Consumers' Interests. 12(28), pp.388 – 403.

Whitman, M., Mattord, H., (2018). Principles of Information Security (6th ed.) Cengage Learning.pp 11-110.

Woretaw, A., & Lessa, L. (2012). Information Security Culture in The Banking Sector in Ethiopia. 5th ICT

2012 Ethiopia Conference, (p. 22 pages). Addis Ababa.

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. Information Systems Frontiers, 18(6), 1205-1215.

APPENDIX A: QUESTIONNAIRE

ADDIS ABABA UNIVERSITY SCHOOL OF COMMERCE

MBIS PROGRAM

(Questionnaire for employees)

Dear Respondent, I am currently a student of Addis Ababa school of commerce, and I am doing my MBIS thesis. On “factors affecting information system security awareness among nib bank employees: knowledge, attitude, perception and training -based analysis”. The purpose of this questionnaire is to gather data regarding the awareness in the case of Nib International Bank. The study is for academic purpose and thus does not affect you in any case. All of your response to the given question would be used for the research and will be kept confidential. Your honest and well-timed response is vital for the success of the study.

Therefore, I kindly request you to respond to each question wisely.

Note:

1. No need of writing your name.

2. If there are multiple options provided, please indicate your selection by circling it and placing a checkmark (√) where applicable.

3. Please return the completed questionnaire in time.

Direction: Please put a choose on the appropriate answer

SECTION A Background Information

General questions regarding the participants profile are given please indicate your choice

Sex

- Male
- Female

Age

- 21-25
- 26-35
- 36-44
- 45&above

Highest education level obtained

- DIPLOMA
- BA/BSC DEGREE
- MA/MSC
- Other ----------

Work experience in the financial industry (in years)

- >1
- 1-3
- 4-6
- 7-9
- 10-13
- Above 14

Field Of Graduate

IT

NON IT

SECTION B KNOWLEDGE, TRAING, PERCEPTION AND ATTITUDE

Knowledge					
Statements	1	2	3	4	5
1. I understand the importance of the CIA triad (confidentiality, integrity, and availability) for information security.					
2. I am confident knowing creating and managing strong passwords according to bank guidelines.					
3. I know and can easily identify red flags of phishing attempts in emails and online interactions.					
4. I am familiar with the bank's policies on data encryption, sharing, and disposal.					
5. I feel comfortable reporting suspicious activity or suspected security breaches to the appropriate channels.					

Attitude					
Statements	1	2	3	4	5
1. Information security is a critical priority for the bank's success.					
2. I do find the bank's information security procedures to be clear and easy to follow.					
3. I am confident in the bank's ability to protect sensitive information from security threats.					

4. I feel comfortable reporting security concerns or violations without fear of reprisal.					
5. I believe that I am likely to encounter a phishing attempt in my work email.					

Perception					
Statements	1	2	3	4	5
1. I believe that I am likely to encounter a phishing attempt in my work email.					
2. The bank's information security policies are clear and easy to understand.					
3. I am personally responsible for maintaining good information security practices.					
4. Following information security procedures hinders my ability to get my job done efficiently.					
5. The bank's current security measures are adequate to protect against cyber-attacks.					

Training					
Statements	1	2	3	4	5
1. The information security awareness training content was clear and easy to understand.					
2.The information security awareness training addressed relevant security threats and procedures					
3. The information security awareness training improved my knowledge of information security best practices.					
4. I found the information security awareness training to be engaging and informative.					
5. The information security awareness training addressed relevant security threats and procedures.					

6.The information security awareness training has influenced me to adopt more secure practices in my daily work.					

Awareness					
Statements	1	2	3	4	5
1. I am aware how serious threats are cyber-attacks to the bank's security.					
2. I am aware and confident in my ability to identify the signs of a malware infection on a work computer.					
3. The bank encourages employees to report any suspicious activity related to information security. I am comfortable discussing such concerns with supervisor or the IT.					
4. Following information security procedures can sometimes feel time-consuming. How much do you agree with this statement					
5. Data breaches can occur when sensitive information falls into the wrong hands. I am well-informed about the bank's policies on data security and appropriate use of work computers.					