COLLEGE OF BUSINESS AND ECONOMICS

SCHOOL OF COMMERCE

THE EFFECT OF TECHNOLOGY, ORGANIZATION, AND ENVIRONMENT FACTORS IN INFORMATION SECURITY PRACTICES ON ORGANIZATIONAL PERFORMANCE: A STUDY OF PRIVATE BANKS IN ETHIOPIA

A THESIS SUMBITTED TO THE OFFICE OF GRADUATE STUDIES OF ADDIS ABABA UNIVERSIT SCHOOL OF COMMERCE FOR THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN BUSINESS INFORMATION SYSTEMS.

By

Nahom Wondiye

Advisor

Meshesha Legesse (PhD)

JUNE 2024

ADDIS ABABA, ETHIOPIA

Approval Sheet

ADDIS ABABA UNIVERSITY SCHOOL OF COMMERCE

MSc IN BUSINESS INFORMATION SYSTEMS

THE EFFECT OF TECHNOLOGY, ORGANIZATION, AND ENVIRONMENT FACTORS IN INFORMATION SECURITY PRACTICES ON ORGANIZATIONAL PERFORMANCE: A STUDY OF PRIVATE BANKS IN ETHIOPIA

By: NAHOM WONDIYE

APPROVED BY BOARD OF

EXAMINERS

Dean, graduate studies	**Signature**
Advisor	**Signature**
External Examiner	**Signature**
Internal Examiner	**Signature**

DECLARATION

I, **Nahom Wondiye**, declare that this research paper, entitled **"THE EFFECT OF TECHNOLOGY, ORGANIZATION, AND ENVIRONMENT FACTORS IN INFORMATION SECURITY PRACTICES ON ORGANIZATIONAL PERFORMANCE: A STUDY OF PRIVATE BANKS IN ETHIOPIA"** is my original work submitted for the award of fulfillment of requirement for Masters of Science (MSc) Degree in Business information systems.

It has not been presented for the award of any degree or other similar titles in any other institutions higher learning to the best of my knowledge, and the resource used have been dully acknowledged.

Addis Ababa University would guarantee to protect the property right of the writer and take full responsibility from its side after the submission of the thesis to the Department.

Declared by:

Name: Nahom Wondiye

Signature:_____

Date: _____

ACKNOWLEDGEMENT

First and foremost, I would like to thank my almighty God for all the blessings and the strength he gives me every day to complete this study, as nothing is possible without him. My sincere thanks go to my advisor, Dr. Meshesha Legesse, for his invaluable guidance and feedback. I also thank my family, especially my father, Wondiye Kebede, for his endless support and encouragement. Additionally, I also appreciate for the academic support rendered to me by Dr. Alazar Ali, finally I thank all the cooperation of the participating banks.

Table of Contents

List of Tables

List of Figures

List of Acronym

ISP	Information Security Practice
ISPR	Information Security Practice towards Organizational Performance
TOE	Technological, Organizational and Environmental (Theory)
ISC	Information Security Culture
OP	Organizational Performance
TF	Technological Factors
OF	Organizational Factors
EF	Environmental Factors
ISTA	Information Security Standards and Awareness
ISSPP	Information Security Systems Policies and Procedures
MSSC	Management Support and Security Commitment
PTA	Perceived Technology Advancement
ISAS	Information Security Awareness and Standards

Abstract

This study examines the determinant factors of information security practices on organizational performance among private banks in Ethiopia. The objective is to assess how technological, organizational, and environmental (TOE) factors influence the effectiveness of information security practices and, subsequently, organizational performance. To achieve this, a framework consisting of TOE factors was proposed. A quantitative research methodology was employed, involving a survey of 140 respondents from 3 private banks in Ethiopia to gather data on organizational performance and the related TOE factors. Multiple regression analysis was used to test the relationships between organizational performance and the identified TOE factors, as well as to assess the reliability and validity of the data. The quantitative approach allowed for a systematic examination of the data, providing statistical evidence of the relationships between the variables. The results indicate that technological, organizational and environmental factors have positive and significant effect on *organizational performance. Specifically, the study found that robust information security practices, supported by Technology, organizational and environmental considerations, lead to improved performance by reducing human errors, internal incidents, and vulnerabilities to social engineering attacks. The findings suggest that adopting comprehensive information security practices is crucial for enhancing organizational performance in the private banks. By analyzing the effect of information security practices using the TOE framework, this research provides valuable insights for strengthening information security measures and ultimately improving the performance of private banks in Ethiopia.*

Keywords: *Organizational performance, Information security practices, TOE factors, Private banks.*

CHAPTER ONE

1.1 Background of the study

Information security was already present before computers, such as encryption, which has been used since humans were able to write (Vacca, 2012). The scenario for information security today is more complex than it was in the past. Thus, the way we handle and secure information has been changed by the introduction of computers and the development of internet technology. The evolving technology and new business arrangements in distributing information have made it vital for all business owners and business management to consider IT security effort (Agosa, n.d.).

Organizations have changed how they operate to improve business performance due to advances in technology (Parsons, 2010). These changes have the potential to increase sales volumes. On the flip side, they have the potential to contribute to profit growth. A company's performance can be affected either positively or negatively by such changes. The internet and ICT, in particular, have made the world more globally connected. Organizations can share information online through the effective use of ICT, as highlighted by Vacca, (2012) people are the target of social engineering assaults, organizations run the danger of losing information to these attacks

According to Alshaikh (n.d.) Information security has become a major focus for organizations over the past 20 years. Companies rely heavily on their IT systems to operate. To stay competitive, organizations need to share data with employees, partners, and customers outside of traditional boundaries (Anderson et al., 2017). As the need for information sharing has grown and new technologies have been adopted, ensuring security has become more difficult. Facing these challenges, organizations implement technical solutions to protect their valuable information assets as they aim to gain advantages through data access while guarding against rising security threats. Maintaining both access and protection is an ongoing challenge in today's digital business environment (Parsons 2010).

The main purpose of information security is to guarantee the confidentiality, availability, and integrity of an organization's information (von Solms and van Niekerk, 2013). According to

Samonas and Coss, (2014) Confidentiality refers to limiting access to authorized individuals only. Availability means ensuring data and systems are accessible when needed and Integrity involves protecting information from unauthorized changes. Securing and safeguarding information assets helps bring structure and governance to the information security function within an organization. Putting measures in place to protect information resources provides organization and management. This allows the information security role to be properly defined and carried out according to good governance principles. The overall goal is to appropriately handle and oversee information using a structured and governed approach (Anderson et al., 2017).

While organizations use technological security measures to bolster protection, relying only on technology is not enough to appropriately manage risk, as the increasing number of reported data breaches shows. According to Alahmari and Duncan, (2020) The growing number of security incidents organizations face demonstrates that technological defenses alone are incapable of successfully mitigating threats. In Addition, as noted by Huang et al., (2023) it shows that viewing information security solely as a technical issue takes to narrow a view of the challenges involved. Genuine risk reduction demands a more comprehensive approach that acknowledges security as both a technical issue and one dealing with human and organizational elements. A holistic method is needed that considers the human and social factors alongside the technological aspects of information security.

Financial Institutes perform a vital function in the economy by facilitating spending and investment (Hassan et al., 2011). However, Levine, (1997) indicates as financial institutions, they are also at risk of failure, which can significantly impact the broader system. Traditionally, the banking sector has been highly regulated regarding information security, privacy, and backups due to the sensitive nature of their data and its importance. However, as suggested by Urbinati et al., (2020) digital transformation accelerates across industries, other organizations are increasingly storing and processing similar types of confidential files electronically. While cyber threats can endanger any business, a major breach or system outage at a large bank in particular could have widespread negative economic effects, as demonstrated during periods of past financial turmoil (Yohannes, 2018).

Implementing effective information security practices is critical for organizations performance, yet poses significant challenges. A major risk is inadequate security management, which can expose the organization to cyber threats, compromising data integrity and confidentiality. As Cremer et al., (2022) explain, failure to comply with regulations can result in fines, while a successful hack of a bank's systems could lead to system unavailability and loss of customer trust and revenue. However, adopting security best practices also faces difficulties. A primary obstacle is lacking a dedicated security budget, as implementing risk management controls is costly (Ernst & Young, 2014).

The Relationship between information security practices and organizational performance is hugely important in the context of Ethiopian private banks. Previous studies, Selamat and Babatunde, (2014) have shown that effective information security measures positively impact organizational performance in Nigerian banks. This can be attributed to improved protection of vital data, decreased risk of security breaches, increased customer trust, and enhanced operational efficiency. Furthermore, the mediating impact of information security culture has been acknowledged by Adebola, (2014) indicating organizations with a strong security practice are more likely to realize better performance outcomes. Therefore, comprehending the relationship between information security practice and organizational performance is critical for in Ethiopia.

To recapitulate, in today's business environment the importance of information security practices and their influence on organizational performance is widely recognized in today's business environment. With the rising issue of cyber threats and potential susceptibility of financial institutions, it is critical to examine the effect between information security activities and organizational performance. Specifically, it intends to examine information security practices and their Effect on organizational performance in order to avoid risks associated with information security failures caused by human error from inappropriate security standards, policies and procedures. By analyzing the effect of information security practice using TOE Framework, this research seeks to provide valuable insights for strengthening information security practices and ultimately enhancing organizational performance in the financial sector.

1.2 Statement of the Problem

Information security has become a critical issue for organizations around the world as they increasingly rely on digital systems and networks to conduct business operations and store sensitive data (Dutta and McCrohan, 2002). Financial institutions in particular face significant information security risks given the private financial data they handle (Al-Bassam and Al-Alawi, 2019). Thus, effective information management highly essential for financial institutes to protect their information asset and maintain trust with customers. Failure to establish good information security practice exposes organizations the following threats; loose of confidentiality such as theft of data; loose of integrity such as virus attack or alteration on files or documents, social engineering attack and lack of availability such as Denial of service (von Solms, 1999).

Information security activities encompass a wide variety of managerial and technical aspects that help foster an organizational information security practice (Schlienger and Teufel, 2003). Specifically, information security practices involve Managerial, technical, and human elements that cultivate security awareness among employees. The focus is on reducing harmful behaviors through the embedding of a robust security practice within organizations (Tanrıverdi and Metin, 2021).

In Cognizant of the problem, Parsons (2010), argued that organizations implement technical security controls to enhance protection. In supporting the above Alahmari and Duncan, (2020) asserted that Technology alone is not enough to properly manage risk, as demonstrated by the growing number of data breaches reported. The increase in security incidents experienced by companies indicates that technological defenses alone are not enough to successfully mitigate threats (Liang and Xue, 2009). This indicates that viewing information security as only a technology issue is an overly narrow perspective of the challenges faced. Thus, this research focus on the managerial perspective of information security that refers to the development and implementations of policies, procedures and control to protect an organization data and asset against potential threats. Managerial aspect of information security also involves identifying potential risk assessing their likelihood and potential impact developing and implementing remediation strategies design to decrease as much as possible.

The absence of proper security management leads to chaos caused by employees' unwillingness to handle security challenges (Parson 2010). Therefore, Information security practices must be established to ensure the proper protection of information assets. This ensures the achievement of organizational objectives and improves organizational performance (Barona and Anita, 2017).The Ethiopian financial system, the focus of this study, is largely dominated by banks, which hold a significant share of assets, deposits, loans, and equity in the sector (Abdu 2022). like all organizations, banks are at risk of disruptions to their information technology systems, which can severely impact their ability to perform basic functions. As Negussie, (2015) suggests managing information security faces several challenges for Ethiopian financial institutions. For instance, lack of awareness and training on information security among employees, inadequate budget allocation for information security, and the absence of a comprehensive information security policy are some of the issues Ethiopian financial institutions must address.

While previous research by Selamat and Babatunde, (2014) established links between information security culture, practice, and organizational performance using a technological, organizational, and environmental (TOE) factors framework. However, there are still gaps in understanding the relationships and effect of information security practices on organizational performance in other country contexts. As digital transformation accelerates in Ethiopia, it is important to understand how key security related factors within these three TOE contexts such as; technological context (Perceived technology Advancement), organizational context (Information Security Awareness, Information security policy and procedure, Perceived management support and commitment, Motivation of the employee), and environmental context (Information security standards). By using this TOE theory, the researcher aims to study these relationships in the Ethiopia context. Studying these relationships through the established TOE model could provide valuable country-specific insights for Ethiopian stakeholders seeking to implement appropriate security measures and manage evolving cyber threats. The findings would also yield helpful knowledge supporting digital development efforts in Ethiopia, as this theoretical framework is yet to be applied in the local context. By minimizing gaps in understanding these precise interactions, the study intends to optimize how security activities can

be designed and resources allocated to realize competitive benefits for organizations operating in Ethiopia.

Few researchers in Ethiopia have Conducted information security; such as Yohannes (2018), has tried to study Assessment of information security incident management Practice in Ethiopian bank, Negussie (2017), has studied about information technology disaster recovery practices of Ethiopian commercial banks, and Asheber (2017), has tried to identify potential challenges in relation to business continuity management in Ethiopian financial institutions, However, these studies did not provide a holistic assessment of information security practices and their impact on organizational performance. Therefore, there remains a lack of comprehensive research evaluating the overall effectiveness of information security practices in Ethiopian banks. there appears to be a lack of holistic research on information security management practices across these organizations.

From the previous discussion, it is clear that the most important initial step in establishing information security is having responsible staff members. Understanding what factors can motivate employees to conscientiously and earnestly carry out information security activities is extremely important. The people responsible for implementing security protocols and safeguarding information assets play a vital foundational role. If they are not appropriately incentivized and compelled to diligently fulfil their duties, then information security cannot be properly developed or managed. Therefore, the critical point to comprehend what drives staff to take information security seriously and put full effort into their related tasks. Figuring out how to incentivize and inspire employees is central to building an effective information security program from the ground up

Thus, this study attempts to assess the effect of information security practices towards organizational performance.

1.3 Research Questions

The preceding Discussion raise the following major research questions for this study

1. What is the effect of the technological factor of information security practices on the organizational performance of private banks?
2. What is the effect of the organizational factor of information security practices on the organizational performance of private banks?
3. What is the effect of the environmental factor of information security practices on the organizational performance of private banks?

1.4 General Objectives

The General objective of this study is to determine the effect of information security practices towards organizational performance of the Ethiopian financial institution, focusing on Private Banks of the nation.

1.4.1 Specific Objectives

To achieve the main goal, the study has the following specific objectives

1. To determine the effect of technological factors of information security practices on the organizational performance of private banks in Ethiopia.
2. To determine the effect of organizational factors of information security practices on the organizational performance of private banks in Ethiopia.
3. To determine the effect of environmental factors of information security practices on the organizational performance of private banks in Ethiopia.

1.5 Significance of the study

The results of this research will provide valuable insights to many groups. For practitioners, identifying the key technological, organizational and environmental factors influencing organizational performance related to information security will help private banks understand the drivers that impact their ability to protect data and systems. The findings can also be used to develop recommendations to strengthen information security practices in areas that are currently inadequate or facing challenges, helping private banks better comply with regulations and

international standards. Researchers could use the study findings to assess risks and management practices in other critical infrastructure sectors that have sensitive digital assets and data. It will add new knowledge to the limited research on this topic in Ethiopia and encourage further study of information security management in organizations. Policy makers can benefit from the results by highlighting issues that require targeted attention or regulatory guidelines to mitigate risks across the financial industry. This could help policymakers in the financial sector to make more informed decisions.

1.6 Scope of The Study

This research covers the effect of information security practices towards organizational performance in Ethiopia private banks using the TOE (technological, organizational, and environmental) framework. Due to cost and time constraints the study only considers private banks located in Addis Ababa, specifically head office. Regarding to content scope, the research examines how aspects within the technological context (Perceived technology Advancement), organizational context (Information Security Awareness, Information security policy and procedure, Perceived management support and commitment, Motivation of the employee), and environmental context (Information security standards) affect information security and the performance of the selected banks.

This research targets to determine information security practice towards organizational performance at private banks from ICT Department staff excluding top-level management. It can be studied from end users' perspective. However, due to time and finance limitations, end users are excluded from the study,

1.7 Definition of Terms

1. Information Security Practice: Refers to the specific activities carried out by organizations to protect information, including implementing controls, training staff, formulating policies and assigning security roles/responsibilities.

2. Information Security Culture: refers to the shared attitudes, values, assumptions and behaviors of organizational members regarding information security policies and practices.
3. Organizational Performance: Refers to outcomes related to productivity, efficiency, profitability and growth achieved by the selected private banks through leveraging resources and meeting strategic objectives.
4. Technological Factors: Refer to perceived technology capabilities/advancement levels present in the studied private banks.
5. Organizational Factors**:** Refer to information security practice, polices, top management support, staff awareness/training programs and perception of security risks present in the studied private banks.
6. Environmental Factors: Refers to adherence to international security standards by the studied private banks.

1.8 Organization of the Thesis

This research is organized in five chapters. It includes:

1. Chapter 1: it introduces the background of Determinant of information security practice towards organizational performance in financial sectors especially in banks. Moreover, it discusses an introduction, statement of the problem, research questions, general and specific objectives, scope and limitations, and significance of the research
2. Chapter 2: in this chapter, provides a review on the models and theories related to information security practices, information security practice and organizational performance.
3. Chapter 3: this chapter describes the research design and methodology used. Thus, the chapter includes, research design, source of data, sampling technique, data collection methods, validity, reliability, data analysis.
4. Chapter 4: in this chapter, the collected data is analyzed, interpreted, described and discussed based on the significance of the key findings in light of what was already known about the research problem.
5. Chapter 5: this chapter concludes the research and provides recommendations depending up on the findings.

CHAPTER TWO

LITRATURE REVIEW

2.1 Introduction

This chapter focuses on reviewing previous literature relevant to the study. The theoretical foundation for this research is based on prior work and findings from scholars in the field of information security practice. To provide more details, a conceptual model depicting the theoretical framework is designed and presented in this chapter. Fundamentally, the chapter examines in depth the concept of technology, organization and environmental theory (TOE theory), along with supporting theories such as security system theory, security policy theory to develop the theoretical framework. These theories will be discussed later in this chapter.

2.2 Information security

Companies utilize various types of security measures such as information security, operations security, production security, personnel security, and computer security. As Singh and Gupta, (2019) describes Information security refers to practices that protect information and information technology systems from risks like loss, misuse, unauthorized disclosure, or damage. Information security professionals are tasked with implementing business processes to safeguard information assets in all forms - whether digital or non-digital, in transit, being processed, or at rest.

As Identified Frangopoulos et al., (n.d.) Information security can be further categorized into two main components - the technical aspect and the social aspect. This study will focus specifically on the social aspect of information security. The reason for this is that many security failures are attributed to human errors.

2.3 Information security Practice

Information security practices refer to the actions and behaviors that take place within an organization to safeguard information (Bulgurcu et al., 2010). Over time, if these security practices are implemented in an acceptable and consistent manner, they will ultimately help promote appropriate security. Also, Amankwa et al., (2018) describes the implication of effective information security practices do not automatically emerge, but rather they develop gradually as employees engage regularly in positive security behaviors and actions as part of their daily work. When these security practices and behaviors are normalized and integrated into the organizational norms and processes in an appropriate way, it leads to the establishment of solid practices for prioritizing information security.

Every organization, including financial institutes, recognizes the importance of information security and also needs to Motivate and encourage their employees to uphold information security concepts and principles through their practices (Camillo, 2017). This will ultimately help create strong information security practices. In the study conducted by Pérez-González et al., (2019) To ensure consistent implementation of security practices, all staff members must recognize security behaviors as part of their regular work. Organizations must create a supportive environment for employees to develop appropriate information security practices to enable this. Whenever this happens, all employees will show a high degree of concern and willingness to secure organizational information and assets through their practices. The aim of this study is to determine the factors that can be used to establish effective information security practices within organizations. In this context, the study defines information security practices as the actions and behaviors regarding information security that guide employees' work within an organization.

2.4 The importance of information security practice

As emphasized by Bulgurcu et al., (2010) The adoption of best security behaviors and actions among all staff within an organization is promoted through information security practices. When employees are not properly trained and guided on security, problems and inconsistencies can arise (Parson 2010). Effective information security practices aid organizations in establishing appropriate norms and processes that enable staff to minimize security errors and failures

(Herath and Rao, 2009). Security awareness programs and ongoing training are provided to address threats and deceptive attacks. As highlighted by Crossler et al., (2013) The improvement of human activities and work processes related to security is a result of developing strong information security practices within an organization, which ultimately enhances organizational performance. In other words, establishing robust information security practices is important for all organizations, including banks, to gain the benefits of improved protection and better overall functioning through consistently secure behaviors implemented across the workforce on a daily basis.

2.4.1 The Relationship between Information Security practice and Organizational Performance

The goal of developing effective information security practices is to safeguard information from inappropriate or unauthorized behavior that could potentially threaten security through the misuse of computer systems (Kayworth and Whitten, 2012). In other words, the aim of information security practices is to ensure the confidentiality, availability and integrity of organizational information. Establishing such practices brings structure and governance to how information security is managed within an organization. It also enables business continuity, compliance with legal requirements, and achieving competitive advantage (Solomon and Brown, 2021). Therefore, while making a profit is primary, establishing information security practices is a secondary necessity to facilitate sustainable profit generation by protecting key data and systems as organizations conduct operations.

On the other hand, the main objective of the organization is to increase sales volume, profit and create a niche for a competitive advantage in the global market. Human behaviors are crucial for improving performance (Anderson et al., 2017). Hence, the need for effective information security practices becomes critical in order to enhance organizational performance over the long-run by guiding all employees to consistently demonstrate secure behaviors and handle information appropriately, this supports both security and business goals.

2.4.2 Establishing Effective Information Security Practice

Information security practices are initially established within an organization through activities aimed at cultivating appropriate behaviors (Zakaria, 2013). Thus, employee actions need to be aligned with effective information security practices.

According to Ernest Chang and Lin, (2007), practices refer to the standards, processes, and guidelines that define how work is performed within a given organizational environment. To develop robust information security practices, all staff members must observe and comply with sound procedures and policies when carrying out any security-related tasks. Understanding what shapes information security behaviors and job functions is crucially important Amankwa et al., (2018) The focus of this study is identifying how to instill practices that prevent non-compliance among employees regarding information security. Determining the drivers of security actions will provide valuable guidance for fostering an environment where protection is ingrained in daily operations.

This study examines how technological, organizational, and environmental factors influence the establishment of information security practices in financial institutions based on prior literature Selamat & Babatunde, (2014); Weill & Ross, (2004); Von Solms, (2000); Barafort et al., (2004). These factors are assessed according to the Technology-Organization-Environment (TOE) framework Tornatzky et al., (1990), which provides a structured way to evaluate adoption influences. Specifically, the technological context comprises perceived technology advancement. The organizational context includes information security awareness programs, policies/procedures, management support, and employee motivation. The environmental context refers to information security standards compliance. Analyzing the impact of these TOE dimensions, including technological perceived capabilities, organizational security measures and programs, and environmental compliance requirements, should offer meaningful insights into developing robust security practices within financial organizations.

2.5 Technological Factors

The use of technologies plays a crucial role in both enabling effective business operations for organizations through tools like mobile devices and introducing new information security

challenges (“Bryan” Jean et al., 2008). As technology becomes more prevalent in storing, processing, and transmitting valuable organizational data, organizations become more dependent on having robust security measures in place (Cascio and Montealegre, 2016). Remote work tools can improve efficiency and flexibility, but they can also create new vulnerabilities in data privacy, access control, and privacy if not properly secured. At the same time, Encryption, firewalls, and intrusion detection systems are essential technology solutions for organizations to protect against unauthorized access and mitigate risk to sensitive information assets in today's digital environment(Pearson, 2013).

However, simply implementing technical security solutions is not enough. Accounting software and information systems can benefit the banking sector by automating processes and providing timely data, inconsistent implementation and failure to meet user needs on accuracy has meant banks have struggled to fully leverage these technologies. Therefore, according to Selamat and Babatunde, (2014) In order to gain competitive advantages and enhance information security, organizations must combine security investments with rigorous implementation and development processes to create solutions that deliver high-quality, user-centric results. By balancing technology and operational implementation, organizations can better utilize new tools while protecting critical information to improve their performance.

2.5.1 Perceived Technology Advancement

The use of information technology has led to major transformations in how Financial Institutes handle and retain information(Melville et al., 2004). IT has also modernized data processing and storage methods. Additionally, telecom networks have enabled beneficial networking of information systems both within individual banks as well as across multiple financial institutions(Yunis et al., 2018).

overseeing information technology capabilities has become one of the most challenging aspects of modern organizations, especially with regards to technical expertise(Ullah et al., 2020). This is due to factors like the growing complexity of electronic business operations, the variety of technology platforms and parts composing an organization's systems, and pressures to cut

expenses while also enhancing workflows in ways that boost profits. Managing the IT infrastructure that supports all aspects of E-business in a cost-effective manner has become more challenging as businesses increasingly move online and rely on sophisticated digital interactions (Masa'deh et al., 2018). Additionally, blending numerous technologies from different vendors introduces management difficulties.

The challenges mentioned emphasize the necessity of information security strategies that consider technological advancement. Having the right IT capabilities enables organizations to implement security measures with efficiency and productivity. Furthermore, technology plays a crucial developing role in the banking industry by increasing sales, improving operations, and achieving cost savings - establishing IT as a wise investment for the future. Therefore(Barras, 1990) indicates IT should be viewed as a way to enhance security practices rather than just an expense. Since technological progress introduces new types of risks, perspectives on development levels must be included in developing comprehensive security practices. Thus, effectively dealing with technology factors results in more robust security positions in the long run. The perceived movement of technologies represents an important aspect that needs to be incorporated into the theoretical basis underlying this research. As tech continues to evolve, so too do perceptions of its evolution, which significantly impacts how organizations approach information security and ultimately achieve their objectives.

2.6 Environmental Factors

Businesses today operate in increasingly complex environments due to global digital transformation and geopolitical uncertainties, as noted by Kling and Lamb (1999). Protecting sensitive data from a diverse range of evolving threats in this context is critical for long-term success, according to Zeng and Koutny (2019). Regulations and political instabilities impact the environments where multinational organizations conduct operations, as highlighted by Zeng and Koutny (2019). As such, information security approaches must consider prevailing conditions to sufficiently address challenges, in line with the perspective of Kling and Lamb (1999).

Adopting internationally recognized information security standards demonstrates commitment to protecting systems and data through established best practices developed via global consensus, as identified by Siponen and Willison (2009) and Humphreys (2008). Compliance with these benchmarks assures stakeholders that adequate controls are implemented according to expertise from an international community, supporting the views of Humphreys (2008). These fosters trust essential for cross-border cooperation, a necessity given prevailing realities, building on the work of Siponen and Willison (2009). Referencing global standards also keeps organizations aware of emerging risks addressed worldwide, aligning with arguments put forth by Humphreys (2008).

Within the TOE framework, the environmental context examines external factors influencing technology adoption, consistent with the framework developed by Tornatzky et al. (1990). Compliance with information security standards strengthens practices by reflecting the value placed on safeguarding information using a worldwide perspective, aligning with Siponen and Willison (2009) and Humphreys (2008). This provides a more comprehensive understanding of diverse environments and enhances the effectiveness of security protocols over time, augmenting the existing literature from Tornatzky et al. (1990).

2.6.1 International Security Standards

Ethiopia has experienced quick advanced change in recent years, with expanding internet penetration and technology selection over different businesses (Kebebe, 2019). However, security challenges stay as organizations collect, handle and store more delicate information online (Gebremichael et al., 2020). Adhering to established frameworks like ISO 27001 is especially critical for Ethiopian businesses looking for to extend regionally and all inclusive, as illustrated in past research (Amankwa et al., 2018; Brenner, 2007). Compliance signals to international partners the appropriate controls and administration are in put to secure shared information systems and client information according to worldwide best practices (Viegas and Kuyucu, 2022).

AS noted by Kebede, (2019) Compliance with international security standards is vital for Ethiopian firms within the banking and financial sector that work inside strict regulatory

systems. Adhering to established benchmarks confirms for domestic regulators that client financial information is adequately protected through implemented controls. Additionally, implementing standardized security practices embraced by communities like ISO can control concerns international banks and investors may have with respect to security risks when partnering with or contributing in Ethiopian financial partners. Over the long term, following to globally recognized frameworks may offer to foreign financial investors looking for wards where consistent security postures enough mitigate emerging threats to shared digital operations and regional ventures (Amankwa et al., 2018; Brenner, 2007). On a national level, targeting compliance with international standards by key sectors could instill confidence in Ethiopia's burgeoning digital economy. When security postures are verified and incidents are minimized through adherence to established frameworks, digital public services and emerging technologies like cloud computing can be further leveraged for socioeconomic development. This thesis will explore how aligning information security practices with global standards can support Ethiopia's digital transformation agenda.

2.7 Organizational Factors

There are several important organizational factors that influence information security practices according to (Hu et al., 2012). These include information security awareness among employees, employee motivation, perceived information security policies and standards, and perceived management support and commitment. Information security awareness is crucial, as staff's understanding of the security posture and individual obligations fosters participation in protective behaviors. Employee motivation plays a role in shaping engagement in secure practices and decision-making. Furthermore, information security policies and standards that are clear and well-perceived and outline expected behavior help guide employees in a positive way.

2.7.1 Information security awareness

Information security awareness is crucial for organizations to protect their data and information assets. It involves creating employees' sensitivity to the threats and vulnerabilities of the system and the recognition of the need to protect data and information (Chen et al., 2006).

According to Lessa et al., (2019) defines information security awareness as the extent to which organizational members understand the level of security required by the organization and their individual security responsibilities." Big organizations are more capable of implementing information security activities than small and medium organizations because they have adequate cash, IT experts, and greater economies of scale.

As noted by Chen et al., (2006) Security awareness and security training programs should be seen as distinct but complementary efforts, not as interchangeable. Effective security training programs require information security awareness. The purpose of raising awareness about security issues among employees is to generate interest and motivation for training. Without adequate awareness of security basics, training programs would likely fail to resonate or drive positive changes in behaviors and actions(Lebek et al., 2014). Therefore, information security awareness and security training initiatives should be thought of as going hand in hand. Awareness precedes and enables training by building fundamental knowledge and awareness of the importance of security topics in employees' minds. The two approaches are most effective when they are sequenced and integrated as interactive components of an overall security practice development strategy within an organization.

To conclude, information security awareness promotes information security efforts within organizations, which ultimately cultivates an information security practice. This then helps guarantee effective systems and decision-making that leads to improved organizational performance overall. As such, information security awareness, the development of an information security practice, and impacts on organizational performance are rightfully incorporated into the theoretical framework underpinning this research. Therefore, exploring the relationships between awareness and organizational performance provides a comprehensive lens through which to analyze the topics targeted by this study.

2.7.2. Perceived Management Support and Commitment

According to Kim et al., (2016) Effective establishment of information security as a norm and practice in organizations requires essential top management support and commitment. Such

endorsement becomes crucial as it enables organizations to enhance their information processing capabilities and remain competitive in the global market.

Organizational performance is significantly affected by perceived management support and employee commitment, particularly in information security management practice. The employee's perception of the organization's value, care, and support for their well-being and development is referred to as perceived management support (Eisenberger et al., 1986). The employee's perception of the organization's value, care, and support for their well-being and development is referred to as perceived management support (Meyer & Allen, 1991). Both Perceived management support and employee commitment have been shown to positively influence various performance outcomes, including increased job satisfaction, reduced turnover intention, and enhanced organizational commitment (Allen and Brady, 1997)

To conclude, in information security management, Perceived management support and employee commitment are particularly crucial. When employees perceive strong management support for information security initiatives, they are more likely to engage in secure behaviors, report suspicious activities, and comply with security policies (Straub & Welke, 2002). Similarly, committed employees are more invested in the organization's success and are thus more likely to adopt information security practices that protect sensitive data and mitigate cybersecurity risks. Therefore, to be effective in information security management programs, it is essential to foster a practice of perceived management support and employee commitment.

2.7.3 Information Security Policy and Procedure

As noted by Sohrabi Safa et al., (2016) discuss that Information security policies and procedures are key tools utilized in information security that highlight the necessity and extent of information protection measures. They are also meant to impact employee conduct by outlining appropriate and inappropriate actions. The policies and procedures delineate the rules, processes, and framework that must be adhered to within organizations(Knapp et al., 2009). They demonstrate the scope of information security and aim to guide employee behavior in positive ways. Policies and procedures are essential mechanisms for defining information security

standards and governing employee choice and task performance by establishing expectations and guidelines to be followed. They provide the structural plans and governance needed to implement security appropriately across the business according to designated requirements and boundaries (Bulgurcu et al., 2010).

The system security policy is the essential element that directs information security efforts from their conception to development, validation, and ongoing operations. The formulation of the policy is crucial for successful security design, implementation, and ongoing assurance (Hong et al., 2003). Weaknesses in the policy have the potential to permeate downstream and negatively impact operations. The security policy provides the overall framework and direction for information protection initiatives from their inception through the entire lifecycle. According to (Knapp et al., 2009) Flaws or gaps in the policy blueprint put the operational viability and reliability of security measures at risk. Therefore, establishing a robust and comprehensive security policy is paramount because Poor policy construction can cause defects to proliferate and impair both implementation and long-term security functionality.

However, for a security policy to be effective, it must clearly outline the protective measures such as employee guidelines for proper and improper actions as well as how violations will be detected (Pahnila et al., 2007). In other words, the security policy is capable of influencing employee behavior to align with upper management's strategic vision and goals for compliance. To maintain an adequate level of assurance over time, it is important to review the policy periodically. It is also important for the policy to include appropriate processes for handling and responding to security incidents and natural disasters. Hiring practices that minimize risks associated with employees should be described as well. Once the system security policy is established, an information security plan can then be developed based on its guidelines. Overall. This rationale justifies including all three aspects - policies/procedures, security practice, and performance outcomes - within the theoretical framework that guides the current research

2.7.4 Motivation of the employee

Providing incentives or rewards to employees for their good work acts as a way to recognize performance and promote order within an organization (Kuswati, 2020). IT system users may not always be aware of the consequences of their actions. There are those who see technology as helping them complete tasks efficiently, while others think it's more of a hindrance than a help (Kalogiannidis, 2021). Because of varying perceptions, an organization must clearly communicate potential threats as well as consequences for failing to properly safeguard information. Spelling out risks and responsibilities helps employees grasp the importance of actively participating in information protection. As Nnaeto and Juliet Anulika, (2018) Recognizing and disciplining users as needed encourages taking security seriously. Overall, outlining repercussions and maintaining accountability helps foster a practice where all individuals contribute to the security objectives of the organization.

Based on the previous discussion, it is evident that cultivating high motivation among employees facilitates information security practices and subsequently develops an information security practice within organizations. This aids in ensuring relevant and trustworthy information, which results in a reliable decision-making process. This continuum leads to enhanced performance as its end result. In other words, a relationship potentially exists between motivating employees, fostering an information security Practice, and improved organizational performance. These interlinking concepts therefore form the basis of the theoretical framework under examination in this research study.

2.8 Information security practice

Practices are understood to be a system of sharing activities, procedures and behaviors affecting groups such as societies, organizations and governments (Lim et al., 2009).According to Pérez-González et al., (2019) Practices are also a dynamic process, which evolves continuously and can be a driver for employees, influencing not just their performance at work but also their commitment to IT security practices. When information security practices become ingrained, it provides motivation for employees to protect sensitive data and systems on an ongoing basis(Alshaikh et al., 2018). Continuous commitment to information security practices fosters consistent adherence to security protocols. This sustained emphasis cultivates long-term

employee loyalty to following these practices, as they understand the benefits of protecting sensitive data for the organization's overall performance. Consequently, robust information security practices become a powerful motivator for employee engagement and a key driver of organizational success. (da Veiga et al., 2020).

An organization's identity, structure, purpose, and agenda are all established by its organizational practices, which serve as the uniting factor. Employee motivation, engagement, and dedication have all been said to be impacted by an organization's practices (Lim et al., 2009). The shared activities and procedures that make up an organization's practices provide the "social glue" that binds members together and guides their priorities, behaviors and decision-making(Alshaikh et al., 2018). When practices emphasize important goals like information security, it can encourage employees to become more committed to supporting those goals through their efforts and involvement (da Veiga et al., 2020). Well-defined practices gives employees an aligned sense of purpose and direction within their roles ((Pérez-González et al., 2019). Therefore, developing positive and influential organizational practices may help spur greater commitment and participation from all members of the company.

In addition, information security practices can be established within an organization by motivating employees through training, adhering to privacy principles, involving staff in security decision making processes like risk analysis, and having management commitment to security initiatives (Lim et al., 2009). This helps socialize employees to acceptable security rules and standards, positively impacting performance, policies, and management effectiveness. However, establishing too rigid of information security practices could potentially cause resistance to new technologies and transformations, as employees become hesitant to embrace changes due to their familiarity with existing practices and protocols. The security practices act as a guide for employee attitudes and behaviors but may hinder an organization's flexibility to transform over time (da Veiga et al., 2020).

Information security practices within an organization can be examined through the lens of the TOE framework (Tornatzky and Fleischer, 1990). The TOE (Technological, Organizational, Environmental) framework suggests Technological, organizational, and environmental factors

influence the adoption of new technologies and practices (Tornatzky and Fleischer, 1990). The technological context is related to the perceived advancement of technology in information security practices Pérez-González et al., (2019) that supports the implementation of practices. Factors like information security awareness are part of the organizational context Alshaikh et al., (2018), Information security policy and procedure within the organization Lim et al., (2009), Perceived management support and commitment da Veiga et al., (2020), and Motivation of the employee. These organizational elements need to be changed to establish security practices. Finally, the Environmental context represents Information security standards in the external environment the organization operates in (da Veiga et al., 2020). Compliance to these standards shapes the need for certain security practices. By considering these TOE elements, organizations can identify the facilitators and barriers to fostering information security practices towards organizational performance. Therefore, this hypothesis is proposed:

2.9 Organizational Performance

The overarching goal of any organization is to boost sales, profits, and carve out a distinctive competitive position in the global marketplace (Kong et al., 2015). As human beings drive whether performance increases or decreases, establishing an information security practice becomes crucial. Developing such helps mitigate risks arising from human factors. However, top management's commitment to information security also plays a catalytic role in addressing risks within the organization. Strong backing and prioritization from leadership can help solve issues stemming from information security threats by fostering the right security mindset across all personnel. When the importance of protecting organizational assets and embracing secure practices is emphasized from the highest levels of management down, it facilitates building a security-centric practice that minimizes vulnerabilities and their negative impacts on business objectives. Therefore, garnering executive support serves as an enabler for minimizing information security risks and their effects on organizational performance (Adebola, 2014).

As noted by Mithas et al., (2011) Information management encompasses more than just operational procedures and processes. Key aspects such as organizational infrastructure, human factors, technology, and information security activities all play a role. Information security

resources are crucial organizational assets that help support the overall mission. Effective information management requires considering the interplay between technical, procedural and human elements. Things like infrastructure, systems, policies and employee behaviors must be aligned for information to be properly handled and protected (Selamat and Babatunde, 2014). This holistic approach recognizes that people and technology are both integral to either enabling or hindering an organization's information security posture and strategic objectives. Resources devoted to information security help organizations safeguard critical data assets and function smoothly.

From the above discussion, it is clear that organizational performance acts as a dependent variable in this research theoretical framework. To be specific the dependent variable is organizational performance.

2.10 Theories related to Information security practice towards organizational performance

The theoretical foundations that help explain the relationship between information security practices and organizational performance are primarily based on the technological-organizational-environmental (TOE) theory. In addition, the security system theory and security policy theory provide further support.

TOE theory looks at how organizational performance is influenced by technological capabilities as well as organizational and environmental factors. It provides a framework for understanding how information security activities interact with these different elements to impact an organization's outcomes.

2.11 Technological, Organizational and Environmental Theory

This study adopts the technological-organizational-environmental (TOE) theory to gain insight into the key factors for success of information security practice and how it ultimately impacts organizational performance in the banking sector. The TOE theory provides a suitable framework for examining how information security practice is shaped by technological

capabilities, organizational aspects like top management support, and external environmental issues within the context of the banking industry. This will help identify important determinants that can strengthen security practice and thereby enhance performance metrics in the banking sector. TOE theory allows a comprehensive understanding of both internal dynamics and external technological/environmental forces influencing information security practice success in banking.

To understand the critical success factors of information security practice and in turn organizational performance in the financial institutes, this study adopts the TOE theory developed by (Tornatzky and Fleischer 1990). The TOE theory that best describes organization$ elements that affect organization in decision making. It consists of three contexts: technological, organizational, and environmental.

The TOE theory consists of three main contexts that influence organizations: technology, organization, and environment. The technological context acknowledges that organizations are impacted by internal and external technological factors. For information security, this includes internal resources and external capabilities to support practices and solutions. The organizational context examines organizational measures such as size, employee motivation, top management backing, policies, awareness, and training programs. The environmental context looks at external forces such as industry standards, governmental regulations, and international security compliance issues.

Empirical research by scholars such as Adebola, (2014), Ifinedo (2011), Intan Salwani et al. (2009), Kraemer and Govindarajulu (2006), Zhu and Kraemer (2005), Zhu et al. (2004, 2003), Thong, (1999), Chau and Tam, (1997) and Iacovou et al, (1995) has validated the application of TOE theory in examining technology adoption. Given its widespread use in information systems studies, TOE theory offers an appropriate framework for the current study. Specifically, the technological, organizational and environmental contexts outlined in TOE theory will be analyzed. The establishment of an effective information security practice is enabled through implementing suitable information security practices. This subsequently allows organizations to

enhance performance, gain a competitive edge, and carve out market positions by satisfying niche demands.

2.12 Security Policy Theory

According to Singh and Gupta, (2019) The security policy theory assists the organizations to establish, implement and maintain its objectives. The security policy theory posits that the establishment of security policies should serve two important functions. Firstly, policies should be able to maintain and assess security requirements while also persuading top management of these needs. Secondly, policies require analyzing information security requirements to properly define practices. In essence, the security policy theory is relevant to this research as information security policies can motivate the implementation of practices. This is done by outlining requirements and gaining leadership endorsement. The applicability of this theory is supported by the research framework incorporating organizational elements like policies and management support from the TOE theory. The framework examines how such internal factors influence security practices and ultimately the development of an effective security practice (Cheng et al., 2013). Therefore, the security policy theory provides theoretical backing for investigating the role of policies in directing security behaviors and controls through the organizational context.

2.13 Security System Theory

According to Hong et al., (2003) Security systems theory refers to a set of concepts and approaches used to describe, examine and develop complex structures or systems related to security. The theory views security as a complex system made up of interconnected and interdependent components. It provides a framework for breaking down security mechanisms, processes, policies and technologies into their constituent parts and analyzing how they interact with and influence each other.

Security systems theory provides a holistic framework for analyzing information security as an interrelated system, enabling improved practice design via understanding relationships between elements. Systems lens strategically examines challenges and solutions, facilitating robust evaluations and advancements. As noted by Soomro et al., (2016) This study leverages this

theory by assessing determinant impacts, with the framework incorporating practices and organizational performance as interdependent, interacting parts of the comprehensive system. Specifically examining influences on practice and performance is guided by viewing them as dependent variables within the overarching organizational system impacted by determinants. Therefore, this theory suitably directs questions regarding determinants' effects in Ethiopia Financial Institutes.

2.14 Related works

Author	Title	Objectives	Methodology	Key Findings	Observed Gaps
Selamat, M.H. and Babatunde, S.O. (2014)	An investigation of the relationship between information security and organizational performance in Nigerian banks.	To investigate the relationship between information security and organizational performance in Nigerian banks.	Quantitative study using questionnaire distributed to ICT staff in banks.	Found a positive relationship between effective information security measures and organizational performance outcomes like improved data protection, decreased risk of breaches, increased customer trust and operational efficiency.	Limited to Nigerian context, more research needed in different geographies.
Negussie, T.F. (2015)	Information technology disaster recovery practices of Ethiopian commercial banks.	To assess challenges in information security management faced by Ethiopian financial institutions.	Interviews and surveys of ICT managers and executives in banks.	Identified issues like lack of security awareness and training, inadequate budgets for security, absence of comprehensive security policies.	Narrow focus on challenges, holistic research on relationships between variables needed in Ethiopian context

Tsedale Yohannes (2018)	Assessment of information security incident management Practice in Ethiopian bank.	To evaluate information security incident management practices in Ethiopian banks.	Case study research design involving interviews and document analysis in selected banks.	Assessed current practices but did not establish links to organizational performance.	Links between security management practices and performance not extensively covered in local Ethiopian context. .
Getnet g/egziabher (2020)	Assessment of information system security management in selected public organizations in Ethiopia: a gap analysis	To evaluate the implementation of Information Security sector Management (ISSM) and find the gap analysis in four federal public organizations in Ethiopia. The study also examined the repercussions based on international ISO standards	a qualitative approach and multiple case study approach to evaluate the Information Security Sector Management (ISSM)	The study found that there were general gaps in ISSM implementation in public sector organizations in Ethiopia The gaps identified included a lack of experienced human resources in the field, inability to implement an IT system, lack of IT policy, lack of training, lack of user-side understanding, and violating rules and regulations.	The study did not consider the potential cultural or social factors that may affect the implementation of ISSM in public sector organizations in Ethiopia. The study did not investigate the effectiveness of the implemented information security management practices in mitigating cyber threats

MACHOGU, JOEL MOKAYA (2019)	Information security management practice and risk exposure Among commercial banks in Kenya	to determine the extent of implementation of information security management practices to determine the risk exposures as a result of not implementing the management practices to determine the relationship between information security management practices and risk exposures in commercial banks in Kenya	descriptive survey targeting Information Security Managers	The study found that most organizations have implemented information security management practices to a great extent and are exposed to information security risks to a small extent	The study was limited to commercial banks in Kenya, and the findings may not be generalizable to other sectors the study did not investigate the effectiveness of the implemented information security management practices in mitigating cyber threats

Table 1 Related works

2.15 The proposed Theoretical framework

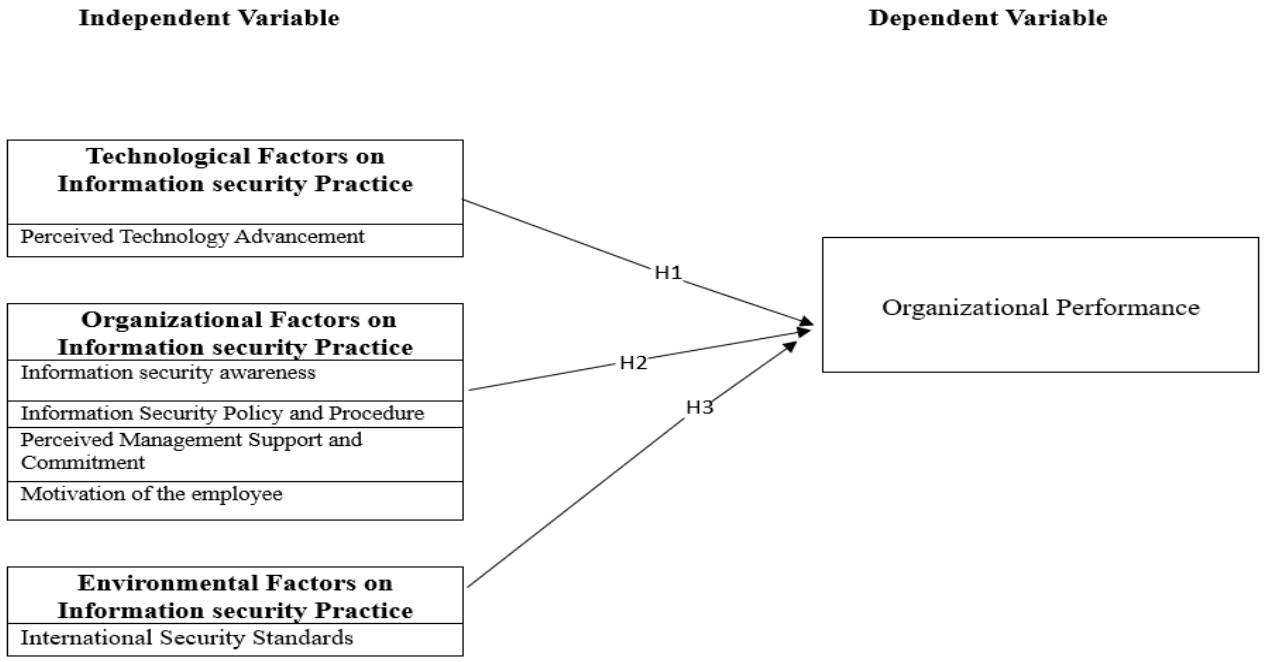

Figure 1 Theoretical framework

Based on the TOE framework discussed above, the following hypothesis are proposed:

H1: Technological factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

H2: Organizational factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

H3: Environmental factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

This chapter describes the research design and methodology which is intended to meet the objectives of this research. Thus, the chapter discusses the research design and techniques used to answer the research questions. It covers the research methodology, data collection methods, data source, validity, reliability and data analysis issues.

3.1 Research Design and Approach

Research design is carried out to provide necessary information on the research and then hypothesize in an accurate manner (Thakur, 2021). Furthermore, Hair et al., (2010; 2009; 2007) stated that Research design is commonly categorized into exploratory, descriptive, and causal designs. Descriptive research design focuses on collecting data to describe a specific research topic using structured questionnaires, interviews, and observations. Likewise, Hair et al., (2010), further divided research into longitudinal and cross-sectional studies. Where data is collected from the same elements at multiple time points it is called cross-sectional studies. Different to that Longitudinal studies allow for the examination of changes over time. Cross-sectional studies are commonly used in social research and involve collecting data at a single point in time to examine relationships and fulfill specific research objectives (Hair et al., 2010; Denscombe, 2010). In the context of this study, a cross-sectional approach is employed to gather information from Ethiopian Private Banks.

This study employed a descriptive research design using a quantitative approach. The primary method of data collection was through the distribution of questionnaires to gather quantitative data from the IT department staff members of selected private banks in Ethiopia. The purpose of this design was to describe the current state of information security practice and its determinants of organizational performance within the context of Ethiopian private banks. By utilizing a

quantitative approach, the study aimed to examine relationships between various factors related to information security practice and fulfill the research objectives. The data collected through the questionnaires was analyzed using descriptive statistics to provide a comprehensive understanding of the research problem and address the research questions effectively (De Vaus, 2011; Dominguez, 2009; Emeka, 2009; Ehikamenor, 2009; Silverman, 2000).

3.2 Study Area

The Ethiopian banking sector consists of 26 private banks, 3 government-owned banks, and 1 national bank. My research focuses on the private banks found In Addis Ababa.

3.3 Study Populations

Table 2 List of private banks in Ethiopia

First generation	1995-2001	Second Generation	2002-2010	Third generation	2011 – up to current time
Bank Of Asbyssinia	1996	Cooperative Bank of Ethiopia	2005	Addis International Bank	2011
Nib International Bank	1999	Oromia International Bank	2008	Global Bank	2012
Awash International Bank	1994	Abay Bank	2010	Enat Bank	2013
Dashen Bank	1995	Berhan International Bank	2010	ZamZam Bank	2021
Hibret Bank	1998	Bunna International Bank	2009	Hijira Bank	2021
Wegagen Bank	1997	Lion International Bank	2006	Amhara Bank	2021
		Zemen Bank	2009	Shabella bank	2021

				Siinqe Bank	2021
				Ahadu Bank	2022
				Goh Betoch Bank SC	2021
				Tsehay Bank	2022
				Tsedey Bank	2022
				Gadaa Bank SC	2023

The Ethiopian banking sector consists of 26 private banks, 3 Government-owned banks, and 1 National bank. Negussie (2017) categorized the private banks in Ethiopia into three generations based on their year of establishment: First generation (1995-2001), Second generation (2002-2010), and Third generation (2011 to present). A purposive sampling method is used to select the first-generation banks. The justification for this is that the number of years these first-generation banks have been implementing IT systems and digital infrastructure, as the researcher assumes, banks operating longer during this early phase have had more time to develop their technical capabilities and expertise in securing technology. In addition to this to satisfy the need for an in-depth study while maintaining representativeness, the researcher selected three of the original six pioneering private banks that are Hibret Bank, Dashen Bank, and Nib Bank, using random sampling method. Examining a randomly selected sample of 3 banks from the earliest established private banks aims to provide insights into the initial approaches to information security adopted during the foundation period of private banking in Ethiopia. These three banks were chosen as they exhibit homogeneity in characteristics relevant to early information security approaches such as comparable IT investment, customer volume, and regulations during 1995-2001.

3.4 Data Collection Methods

This study utilized questionnaires as the primary method for data collection. The questionnaires consisted of closed-ended questions, and a 5-point Likert scale was selected to measure attitudes. The questionnaire was adopted from the study conducted by Nguyen et al. (2022) and adapted to fit

the specific context of this research. The Likert scale was chosen as it provided a balanced number of response options, ensuring reliable measurement and minimizing respondent confusion or indifference, as suggested by Likert (1932) and supported by subsequent research (Preston & Colman, 2000; Jaber, 2017). The questionnaires were distributed to the IT department staff members within the sampled bank to gather their responses.

This study collected quantitative data from a total of 140 IT professionals across Dashen Bank (55 professionals), Hibret Bank (44 professionals), and Nib Bank (41 professionals) using a census method. The researcher used census method due to the manageable population size of the sampled banks and that allowed for the distribution of standardized closed-ended questionnaires to each professional. The questionnaires encompassed two sections, with the first section collecting demographic data and the second section addressing the core research questions in an objective and detailed manner through closed-ended questions. After receiving the required number of responses, the full dataset underwent statistical analysis to determine key relationships.

For this purpose, the general organogram of respective sampled private banks are found below the table.

Table 3 General Organizational Structure

Job Category	Level	Specific Title	Research Method to be Used
	Top Level Managers	Chief Information Technology Officer	
	Middle level Managers	Director, Applications Development & Support Department	
		Director, IT Infrastructure Department	
		Director, Cyber Security Department	
		Director, Analytics and Database Management Department	
		Director, Digital Channels & Platform Department	
		Senior Manager, IT Service Delivery	

IT Department		Application Development and Support	160 Questioners
		User Services	
		Network & Systems	
		End-User Services	
		Security Operations	
		Data Protection and Management	
		Digital Channels	

3.5 Data Analysis Technique

In this research, quantitative data was collected through a questionnaire distributed to IT department staff members of selected private banks. The collected data was analyzed using descriptive statistics such as frequency counts, percentages, and mean scores. Additionally, inferential statistics, specifically multiple regression analysis, were employed to examine the relationship between the dependent variable and independent variables. The findings were addressed through the utilization of tables, graphs, charts, means, standard deviation and percentages. To facilitate the analysis, the researcher utilized the Statistical Package for Social Science (SPSS) version 26 software. This software enabled the researcher to conduct both descriptive and inferential statistical analyses, providing a comprehensive understanding of the collected data.

3.6 Ethical Consideration

The study was conducted with ethical responsibility in mind. The researchers informed the participants about the purpose of the study and how the collected information would be used. Information gathering was done confidentially by the researchers. Respondents' identities were kept anonymous so that participants felt comfortable and secure expressing their ideas freely. Anonymity of the respondents was maintained to ensure confidentiality. The researchers made sure

the participants understood how their information would be handled to obtain truly voluntary participation.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.1 Introduction

This chapter presents the findings from a survey given to IT professionals from three private banks in Ethiopia. The responses were analyzed using the Statistical Package for the Social Sciences (SPSS) software version 26. Both descriptive and inferential analyses are presented in this chapter. Descriptive analysis was employed to summarize key characteristics of the respondents, while multiple linear regression was used to examine the relationships between variables. By integrating these analytical methods, the chapter offers a holistic understanding of the research objectives.

4.2 Data screening and data cleaning

Data screening and cleaning were conducted prior to analysis. Data screening is the process of inspecting data for errors and correcting them, while data cleaning refers to identifying incomplete, incorrect, or inaccurate records and then replacing, modifying, or deleting the dirty or coarse data (Wu, 2013). A total of 160 questionnaires were distributed across Dashen Bank, Hibret Bank, and Nib Bank, of which 145 were returned for a response rate of 90.625%. However, 5 questionnaires were not fully completed and thus discarded. Therefore, the number of questionnaires suitable for analysis was 140, representing a final response rate of 87.5%.

4.3 Reliability Test

The reliability statistics revealed that the scale displayed a high level of consistency. A Cronbach's alpha value of 0.70 or above is commonly used as the minimum threshold for a reliability test. George and Mallery (2003) state that alpha should exceed 0.7 to consider the instrument reliable. The researcher conducted a pre-test of the questionnaires which yielded 0.901. The following tables depicts results regarding the reliability of the instrument.

Case processing summary: **Technological Factors**

		N	%
Cases	Valid	140	100.0
	Excluded[a]	0	0
	Total	140	100.0

Cronbach's Alpha	N of Items
.863	5

Llist wise deletion based on all variables in the procedure.

Case processing summary: **organizational factor**

		N	%
Cases	Valid	140	100.0
	Excluded[a]	0	0
	Total	140	100.0

Cronbach's Alpha	N of Items
.904	10

Llist wise deletion based on all variables in the procedure.

Case processing summary: **Environmental Factor**

		N	%
Cases	Valid	140	100.0
	Excluded[a]	0	0
	Total	140	100.0

Cronbach's Alpha	N of Items
.733	4

Llist wise deletion based on all variables in the procedure.

Case processing summary: **organizational performance**

		N	%
Cases	Valid	140	100.0
	Excluded[a]	0	0
	Total	140	100.0

Cronbach's Alpha	N of Items
.813	3

Variable	Classification Of Variable	Cronbach's Alpha Dasen Bank Frequency	Hibret Bank Frequency	Nib Bank Frequency	No of Item Total Frequency	Percent	Valid Percent	Cumulative Percent
Technological Factors		.863			5			

Organizational Factor	.904	10
Environmental Factor	.733	4
Organizational performance	.813	3
Overall Reliability	**.901**	**22**

Llist wise deletion based on all variables in the procedure.

Table 4 Cronbach's Alpha coefficients (Reliability test)

Source: own research result, 2024

4.4 Demographic Characteristics of Respondents

The demographic characteristics are presented in the table below, as categorized by sampled bank (Dasen Bank, Hibret Bank, and NIB Bank), age, sex, education level, training provision, and certifications of the respondents.

Table 5 Demographic Characteristics of Respondents

Sex of Respondent	Female	12	10	7	29	20.7	20.7	20.7
	Male	43	34	34	111	79.3	79.3	100
	Total	**55**	**44**	**41**	**140**	**100**	**100**	
Age	18-25	11	9	7	27	19.3	19.3	19.3
	26-35	33	28	25	86	61.4	61.4	80.7
	36-44	11	7	9	27	19.3	19.3	100
	Total	**55**	**44**	**41**	**140**	**100**	**100**	
Educational Level	BA/BSC Degree	38	32	24	94	67.1	67.1	67.1
	MA/MSC	17	12	17	46	32.9	32.9	100
	TOTAL	**55**	**44**	**41**	**140**	**100**	**100**	
Work Experience	1-3	24	22	16	62	44.3	44.3	44.3
	4-6	19	13	12	44	31.4	31.4	75.7
	7-9	6	6	11	23	16.4	16.4	92.1
	10-13	6	3	2	11	7.9	7.9	100
	Total	**55**	**44**	**41**	**140**	**100**	**100**	
Training	Yes	47	36	34	117	83.6	83.6	83.6
	No	8	8	7	23	16.4	16.4	100
	Total	**55**	**44**	**41**	**140**	**100**	**100**	
Certifications	Yes	36	28	20	84	60	60	60
	No	19	16	21	56	40	40	100
	Total	**55**	**44**	**41**	**140**	**100**	**100**	

Source: own research result, 2024

As shown in the table 7 the demographic analysis of Dashen Bank's respondents shows a predominantly male population, with females representing approximately 21.8% of the sample. The majority of respondents fell within the 26-35 age group, with 20% aged 18-25 and 20% aged 36-44. The majority of respondents (69.1%) held a BA/BSC degree, while 30.9% possessed an MA/MSC degree. In terms of work experience, 43.6% had 1-3 years, 34.5% had 4-6 years, 10.9% had 7-9 years, and 10.9% had 10-13 years. Notably, 85.5% of respondents had received training, and 65.5% held certifications, indicating a strong emphasis on professional development.

The demographic composition of Hibret Bank's respondents was predominantly male, with females making up approximately one-quarter of the sample. The majority of respondents were aged 26-35, followed by smaller proportions of respondents in the 18-25 and 36-44 age brackets. The majority of respondents held a BA/BSC degree, while a significant proportion also possessed an MA/MSC

degree. In terms of work experience, half of the respondents had 1-3 years, nearly a third had 4-6 years, and smaller proportions had 7-9 and 10-13 years. Additionally, the majority of respondents had received training and possessed certifications, it shows a strong focus on professional development within the organization.

Nib Bank's respondents were predominantly male (82.9%), with a smaller percentage of females (17.1%). The majority of respondents were aged 26-35 (61%), followed by smaller proportions of respondents in the 18-25 and 36-44 age group. The majority of respondents held a BA/BSC degree (58.5%), while 41.5% had an MA/MSC degree. In terms of work experience, 39% had 1-3 years, 29.3% had 4-6 years, 26.8% had 7-9 years, and 4.9% had 10-13 years. Additionally, 82.9% of respondents had received training, but only 48.8% possessed certifications, indicating a high level of training but a lower certification rate compared to other banks.

4.5 Descriptive Analysis

This descriptive analysis examines factors that related to technology practices, organizational practices, and environmental practices. It utilizes the measurement standards established by Phile and Akmalih (2009) to assess these different factors. Using the average cutoff methodology, scores above 3.79 represent high levels of practice of the technology, organizational, and environmental practices, scores from 3.40-3.79 indicate moderate levels of practice, and scores below 3.40 signify low levels of practice.

Table 6 Information Security practice - Technological Factor (N=140)

No	Technological factor Items	Mean	Std. deviation
1	your existing IT infrastructure supports secure and compliant business operations.	4.10	.742

2	The technical skills of your IT staff and capabilities of your technologies equip the organization to prevent, detect and respond to security threats.	4.04	.767
3	The level of integration and collaboration between technology and security teams strengthen security defenses and performance	4.07	.746
4	Investment in new security technologies improves organizational performance.	4.21	.707
5	The bank's technological readiness enables secure digital services.	4.14	.745
	Grand Mean	4.112	

The descriptive analysis conducted in this study assessed the technology factor based on responses from 140 participants. The analysis followed the measurement standards established by Phile and Akmalih (2009), where scores above 3.79 indicate high levels of practice in technology, organizational, and environmental factors. Within the technology factor dimension, all the mean scores for the different items exceeded this threshold, indicating a strong level of practice. Respondents expressed positive perceptions regarding the organization's technological capabilities, as evidenced by the agreement that the existing IT infrastructure supports secure and compliant business operations and that the technical skills and capabilities of the IT staff equip the organization to prevent and respond to security threats. Additionally, the integration and collaboration between technology and security teams were perceived to strengthen security defenses and performance. Moreover, investment in new security technologies and the organization's technological readiness for secure digital services were also positively rated. These findings provide valuable insights into the organization's technological practices, highlighting areas of strength and potential opportunities for further improvement.

Table 7 Information Security practice - Organizational Factor (N= 140)

No	Organizational factor Items	Mean	Std. deviation
1	Security awareness training improves employee technical skills and	4.40	.855

	ability to support secure organizational operations.		
2	Clear security policies and procedures streamline technology governance and compliance with requirements.	4.29	.884
3	Management commitment to technology budgeting optimizes controls and infrastructure defending critical systems	3.98	.971
4	Adherence to information security policies and protocols as part of employee performance evaluations contributes to more secure and productive use of technology by staff.	4.14	.819
5	Regular communication of established security incident response procedures improves information security awareness and preparedness across the organization.	4.29	.782
6	Involving security and IT teams in collaborative planning and policy development encourages buy-in and shared accountability for maintaining information security standards	4.01	.768
7	Gathering inputs from all business units helps drive management commitment to align security spending with strategic needs and operational requirements.	3.99	.861
8	Providing training and resources to build internal security expertise ensures policies and technologies are properly implemented and managed throughout the organization	4.28	.823
9	Conducting regular risk assessments and sharing results helps update security protocols to address emerging threats to business operations	4.28	.769
10	Promoting a security-aware culture fosters cross-team collaborations that strengthen implementation of measures protecting sensitive data and systems.	4.34	.595
	Grand Mean	4.10	

Based on the descriptive analysis conducted, the respondents hold a positive perception of the organizational factors related to information security. The mean scores ranging from 3.98 to 4.40, with a grand mean of 4.10, indicate effective practices in areas such as security awareness training,

clear policies and procedures, management commitment to technology budgeting, adherence to information security policies and protocols, regular communication of security incident response procedures, involvement of security and IT teams in planning, gathering inputs from all business units, providing training and resources for internal security expertise, conducting regular risk assessments, and promoting a security-aware culture.

Table 8 Information Security practice - Environmental Factor (N= 140)

No	Environmental factor Items	Mean	Std. deviation
1	Regulatory certification requirements for security systems and practices improve technical controls, governance and incident response supporting secure operations	4.09	.709
2	Alignment with global security practices through regional cooperation strengthens protection of critical data and infrastructure defending the organization.	4.15	.688
3	Adherence to national security strategies harmonizes technical defenses and roles/processes benefiting compliant operations.	4.15	.562
4	Benchmarking security controls, access management and platform resilience with peers in the Ethiopian banking sector fuels continuous improvement.	4.02	.651
	Grand Mean	4.1025	

The descriptive analysis conducted on the environmental factors reveals a positive perception among respondents. The mean scores ranging from 4.09 to 4.15, with a grand mean of 4.1025, indicate the effectiveness of practices related to regulatory certification requirements, alignment with global security practices, adherence to national security strategies, and benchmarking security controls. These findings highlight the organization's strong focus on maintaining secure operations, harmonizing technical defenses, and continuous improvement.

The relatively consistent standard deviation scores, ranging from .562 to .703, suggest a consensus among respondents regarding these environmental factors. Overall, these results provide valuable

insights for further research and decision-making to enhance the organization's management of environmental factors. The organization can leverage these findings to strengthen its practices and ensure the protection of critical data and infrastructure, in alignment with global standards and national security strategies.

Table 9 Information Security practice - organizational performance (N= 140)

No	Organizational performance Items	Mean	Std. deviation
1	The implementation of new technology has positively impacted the performance of the organization	4.18	.859
2	The organizational structure and processes significantly contribute to the performance of the organization	4.23	.790
3	External factors have a significant influence on the performance of the organization.	4.14	.878
	Grand Mean	4.183	

The descriptive analysis conducted on organizational performance reveals that the respondents hold a positive perception of the impact of various factors on the organization's performance. The mean scores ranging from 4.14 to 4.23, with a grand mean of 4.183, indicate the effectiveness of new technology implementation, organizational structure and processes, and the influence of external factors. These findings emphasize the organization's ability to leverage technology, optimize its structure, and effectively navigate external factors to drive performance.

The relatively consistent standard deviation scores, ranging from .790 to .878, suggest a consensus among respondents regarding the positive influence of these factors on organizational performance. Overall, these results provide valuable insights for further research and decision-making to enhance organizational performance. The organization can capitalize on the benefits of new technology, optimize its structure and processes, and effectively manage external factors to drive continued success and achieve its performance goals.

4.6 Multiple Regression Analysis

There are some assumptions that are required to provide valid results in regression analysis. These assumptions must be met in order to develop a multiple regression model that accurately predicts relationships between independent and dependent variables.

4.6.1 Sufficient Number of Observation

To appropriately examine the relationships between the independent and dependent variables, there is a general guideline for the minimum sample size needed. According to Mooi & Sarstedt (2011), the recommended formula is that the number of observations should be at least 50 plus 8 times the number of independent variables (k). In this study with 3 predictor variables, using the formula of 50 + 8k, the threshold sample size required to conduct regression analysis is 50 + 8*3 = 74 observations. Thus, in this research 140 observations were collected. Therefore, the current sample size meets and exceeds this rule-of-thumb benchmark for multiple regression testing with 3 independent variables.

4.6.2 Testing Multicollinearity

Collinearity can be evaluated by calculating tolerance or the Variance Inflation Factor (VIF). A tolerance level below 0.10 indicates potential issues with collinearity, either between two variables or multicollinearity amongst multiple variables. The VIF is simply the reciprocal of tolerance, so a VIF above 10 also suggests collinearity may be problematic. According to Mooi and Sarstedt (2011), this tolerance and VIF statistical checks can detect if collinearity is present between predictor variables in a regression model. As shown in Table 12, none of the variables have a tolerance below 0.10 or a VIF exceeding 10. Therefore, there does not appear to be any concerning multicollinearity between the variables included in the analysis.

Table 10 Collinearity Statistics

Model	Collinearity Statistics	
	Tolerance	VIF
Technological Factor	0.854	1.171
Organizational Factor	0.794	1.259
Environmental Factor	0.889	1.125

a. Dependent Variable: Organizational Performance

Source: own research result, 2024

4.6.3 Checking for Linearity

Linearity refers to the degree to which the change in the dependent variable is related to the change in the independent variables. To determine whether the relationship between the dependent variable (organizational performance) and the independent variables (technological factors, organizational factors, and environmental factors) is linear, plots of the regression residuals were analyzed using SPSS V26 software.

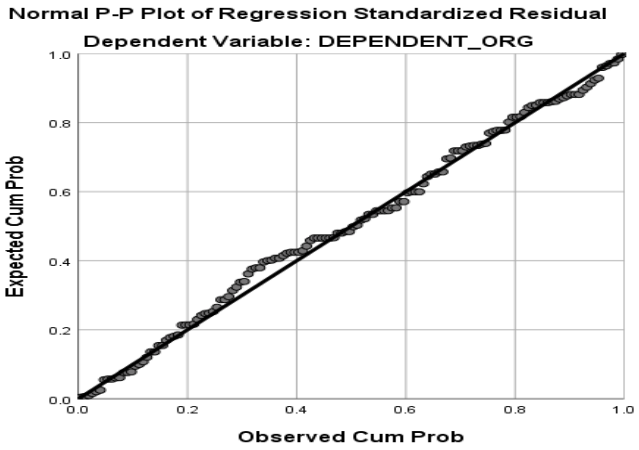

Figure 2 Linearity test

Source: own research result, 2024

From the figure 2 the researcher's assumptions, the Normal P-P Plot indicates the linearity assumption is satisfied for the regression model with the dependent variable (organizational performance) The close alignment of data points to the diagonal line suggests normally distributed residuals and a linear relationship between the dependent and independent variables, confirming the researcher's assumptions and the model's appropriateness.

4.6.4 Homoscedasticity

The homoscedasticity test examines whether the residuals are evenly distributed or if there is an indication of unequal variances, also known as heteroscedasticity. This test was conducted to evaluate the presence of heteroscedasticity in the problem being tested.

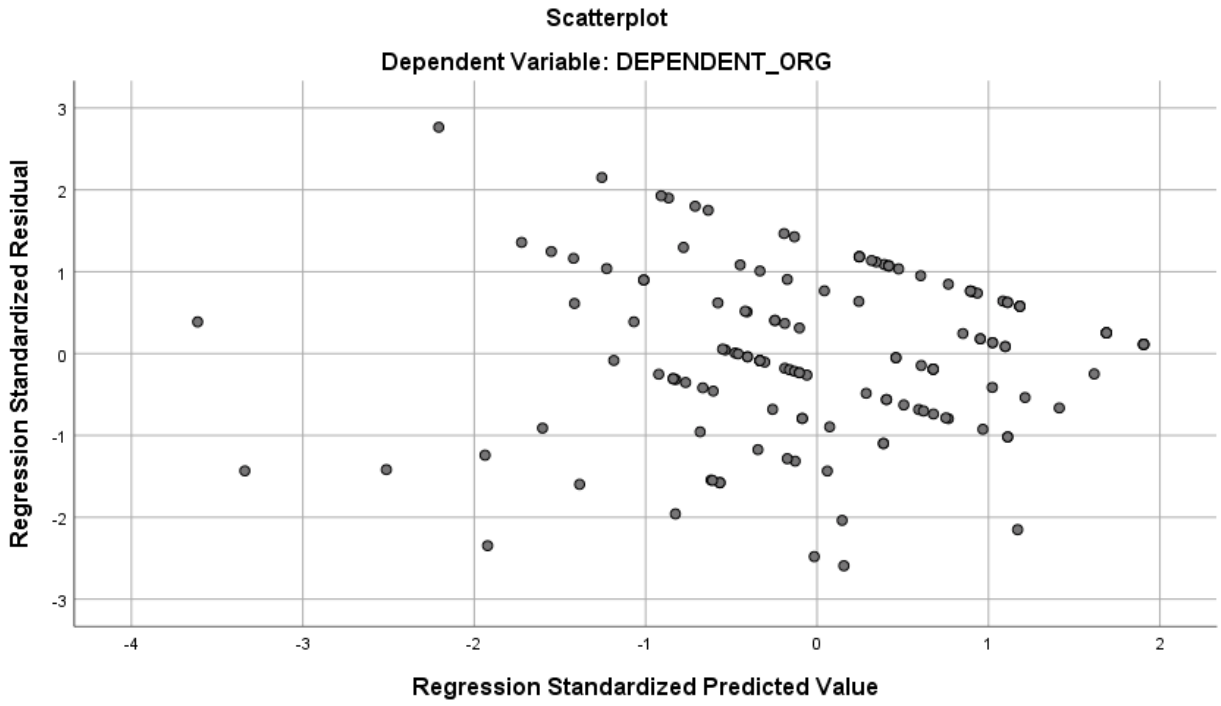

Figure 3 the scatter plot of Homoscedasticity

Source: own research result, 2024

Figure 3 above indicates a random distribution of residuals around the horizontal axis, without a clear pattern. This suggests that the residuals have a constant variance across all levels of the independent variables, which supports the assumption of homoscedasticity.

4.6.5 Checking Normality

Linear regression analysis requires that all variables follow a multivariate normal distribution. This assumption can be effectively verified through the examination of a histogram with a superimposed normal curve or a Q-Q-Plot. According to the fundamental assumptions of Classical Linear Regression Models, the variables should conform to a normal distribution.

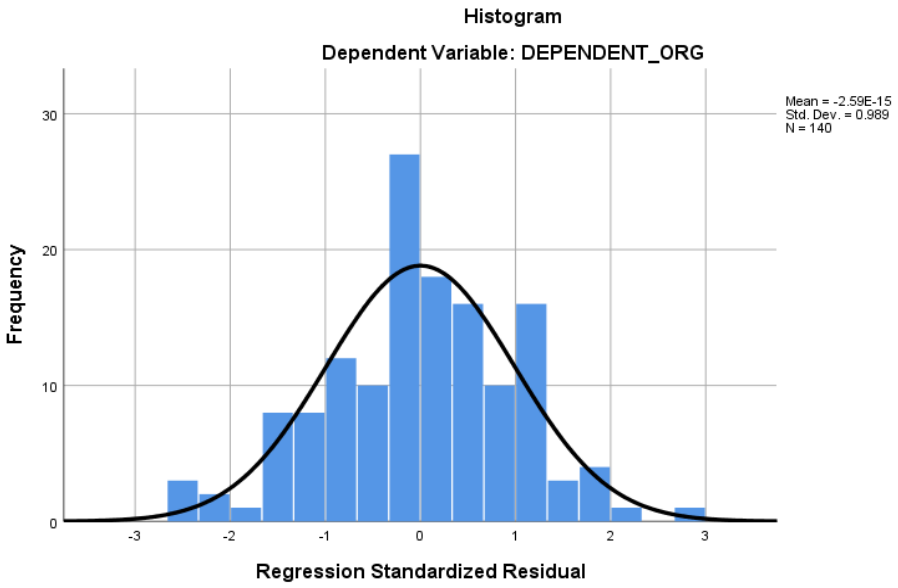

Figure 4 checking Normality

Source: own research result, 2024

Figure 4 shows a bell-shaped curve resembling a normal distribution for the regression standardized residuals of organizational performance It is symmetrical and centered around zero,

indicating normality and aligning with the researcher's assumption. This suggests that the regression model is suitable for the data.

4.7 Regression Analysis

Regression analysis is a widely utilized technique in information security, enabling researchers to examine the relationships between a single independent variable and a dependent variable. According to Mooi and Sarstedt (2011), in this context, the dependent variable typically represents organizational performance, while the independent variables are the TOE (Technology, Organization, and Environment) factors.

Table 11 Variables Entered/Removed

Model	Variables Entered	Variables Removed	Method
1	Technological Factor, organizational Factor, Environmental Factor		Enter

a. Dependent Variable: Organizational Performance

b. All requested variables entered.

Source Own Survey

Table 12 Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.440a	.298	.283	.60881
a. Predictors: (Constant), Environmental Factor, Technological Factor, Organizational Factor				

From the model summary result, it can be seen that the independent variables explain a significant portion of the variance in the dependent variable, organizational performance. Specifically, the R Square value of 0.298 indicates that approximately 29.8% of the variance in organizational performance is explained by the environmental factor, technological factor, and organizational

factor. According to Cohen (1988), an R Square value of around 0.30 represents a moderate level of significance in social science research.

Table 13 ANOVA Table

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	21.441	3	7.147	19.282	.000[b]
	Residual	50.409	136	.371		
	Total	71.850	139			
a. Dependent Variable: Organizational performance						
b. Predictors: (Constant), Environmental Factor, Technological Factor, Organizational Factor						

The ANOVA table provides valuable insights into the overall significance of the regression model. With a significance value of the F statistic less than $p<0.05$ at 0.000, the model is deemed statistically significant. This indicates that the combined predictors (technological l factor, organizational factor, and environmental factor) have a significant influence on organizational performance.

Based on the known constant and beta values presented in the table, the regression model can be formulated

Coefficients							
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	**Decision**
		B	Std. Error	Beta			
1	(Constant)	.196	.537		.364	.002	
	Technology Factor	.340	.092	.282	3.701	.000	**Pass**
	Organizational Factor	.285	.097	.237	2.941	.004	**Pass**
	Environmental Factor	.340	.114	.231	2.966	.004	**Pass**
a. Dependent Variable: organizational performance							

The study examined the effect of three factors of technological, organizational, and environmental on organizational performance. The results showed that all three factors had a significant effect on performance, with the technological factor having the strongest positive relationship. The standardized coefficients (Beta) further highlighted the importance of these factors, with the

technological factor having the strongest positive relationship with performance (Beta = 0.282), followed by the organizational factor (Beta = 0.237) and the environmental factor (Beta = 0.231).

The significance levels (p-values) for the technological factor ($p < 0.001$), the organizational factor ($p = 0.004$), and the environmental factor ($p = 0.004$) were all below the conventional threshold of 0.05, indicating that these predictors are statistically significant. This suggests that there is a real and meaningful relationship between these factors and performance. These findings provide valuable insights into the factors that influence organizational performance, and suggest that organizations should consider these factors when making strategic decisions.

4.8 Hypotheses Testing

In this section, the proposed hypotheses were tested and the results are presented. The hypotheses that were examined are as follows

H1: Technological factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

H2: Organizational factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

H3: Environmental factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

H1: Technological factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

The regression analysis results **support H1.** The technological factor, as indicated by perceived technology advancement, has a significant positive relationship with organizational performance. This is reflected by a standardized coefficient (Beta) of 0.282 and a p-value of 0.000, which is well below the conventional threshold of 0.05. This suggests that improvements in technological factors,

particularly perceived technology advancement, are associated with enhanced organizational performance in the context of information security practices.

H2: Organizational factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

The regression analysis results also **support H2**. The organizational factors, which include information security awareness, information security policy and procedure, perceived management support and commitment, and motivation of the employee, show a significant positive effect on organizational performance. This is evidenced by a standardized coefficient (Beta) of 0.237 and a p-value of 0.004 and also it indicates that better organizational factors, such as strong information security policies and procedures, management support, employee motivation, and security awareness, are significantly correlated with improved organizational performance in information security practices.

H3: Environmental factors of information security practices have a positive and significant effect on the organizational performance of private banks in Ethiopia.

The regression analysis results also **support H3**. The environmental factor, represented by adherence to international security standards, has a significant positive effect on organizational performance. This is evidenced by a standardized coefficient (Beta) of 0.231 and a p-value of 0.004. This implies that favorable environmental factors, particularly the implementation of international security standards, contribute significantly to organizational performance in the realm of information security practices.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the key findings from the data analysis, draws conclusions in relation to the research objectives and offers recommendations for practice and future research. The research focused on understanding the effect of technological, organizational, and environmental factors on the information security practices in three private banks in Ethiopia, utilizing data from 140 valid survey responses.

5.2 Summary of Findings

5.2.1 Demographic Characteristics

The demographic analysis of respondents from Dashen, Hibret, and Nib Banks shows several key findings. The majority of respondents were male: 78.2% at Dashen, 77.3% at Hibret, and 82.9% at Nib. The predominant age group was 26-35 years: 60% at Dashen, 63.6% at Hibret, and 61% at Nib. Most respondents held a BA/BSC Degree: 69.1% at Dashen, 72.7% at Hibret, and 58.5% at Nib. Regarding work experience, many had 1-3 years: 43.6% at Dashen, 50% at Hibret, and 39% at Nib. Training levels were high, with 85.5% at Dashen, 81.8% at Hibret, and 82.9% at Nib having received training. Certification levels varied, with 65.5% at Dashen, 63.6% at Hibret, and 48.8% at Nib. Overall, the respondents were relatively young, educated, and well-trained.

5.2.2 Reliability of the Measurement Instruments

The reliability statistics revealed that the measurement instruments exhibited a high level of consistency. The Cronbach's alpha values for the various factors were as follows: Technological

Factors (0.863), Organizational Factor (0.904), Environmental Factor (0.733), and Organizational Performance (0.813). The overall reliability of the instrument was 0.901, indicating strong internal consistency and reliability.

5.2.3 Descriptive Analysis

The descriptive analysis examined factors related to technology practices, organizational practices, and environmental practices. The mean scores for the technological factor items ranged from 4.04 to 4.21, with a grand mean of 4.112, indicating a high level of practice in this area. For the organizational factor, the mean scores ranged from 3.98 to 4.40, with a grand mean of 4.10, indicating effective practices. The environmental factor had mean scores ranging from 4.02 to 4.15, with a grand mean of 4.1025, suggesting strong practices in maintaining secure operations and aligning with global and national security standards. Finally, the mean scores for organizational performance ranged from 4.14 to 4.23, with a grand mean of 4.183, indicating a positive perception of the effect of the TOE factors on the organization's performance.

5.2.4 Regression analysis

This section presents the results of the regression analysis,

1. Organizational Factors of private banks has positive and significant effect on organizational performance towards information security Practice The result of this finding is in line with previous studies made by Selamat and Babatunde, (2014) along with additional studies by Adebola (2014), Ifinedo (2011), Intan Salwani et al. (2009), Kraemer & Govindarajulu (2006), and Zhu & Kraemer (2005).
2. Environmental Factors of private banks has positive and significant effect on organizational performance towards information security Practice The result of this finding is also in line with previous studies of the Selamat and Babatunde, (2014) along with additional studies by Adebola (2014), Ifinedo (2011), Intan Salwani et al. (2009), Kraemer & Govindarajulu (2006), and Zhu & Kraemer (2005).

3. Technological Factors of private banks has positive and significant effect on organizational performance towards information security Practice The result of this finding is also in line with previous studies of the Selamat and Babatunde (2014), along with additional studies by Adebola (2014), Ifinedo (2011), Intan Salwani et al. (2009), Kraemer & Govindarajulu (2006), and Zhu & Kraemer (2005).

5.3 Conclusion

In this section, the researcher summarized the key findings related to the effects of technological, organizational, and environmental factors on organizational performance in information security practices.

1. The technological factors, including the existing IT infrastructure, technical skills of IT staff, integration and collaboration between technology and security teams, investment in new security technologies, and technological readiness for secure digital services, have a significant positive effect on organizational performance in information security practices. Advancements in these technological factors are associated with enhanced organizational performance.
2. The organizational factors, encompassing security awareness training, clear policies and procedures, management commitment to technology budgeting, adherence to information security policies and protocols, regular communication of security incident response procedures, involvement of security and IT teams in planning, gathering inputs from all business units, providing training and resources for internal security expertise, conducting regular risk assessments, and promoting a security-aware culture, have a significant positive effect on organizational performance in information security practices.
3. The environmental factors, including regulatory certification requirements, alignment with global security practices through regional cooperation, adherence to national security strategies, and benchmarking security controls with peers in the Ethiopian banking sector, have a significant positive effect on organizational performance in information security practices.

4. The combination of technological, organizational, and environmental factors explains a significant portion of the variance in organizational performance, highlighting the importance of considering these factors in strategic decision-making processes.

5.4 Recommendations

Organizations should prioritize investments in technological advancements like upgrading IT infrastructure, enhancing IT staff skills, fostering technology-security team collaboration, and adopting new security technologies to improve organizational performance in information security practices. Additionally, by upgrading infrastructure, enhancing staff expertise, promoting collaboration, and adopting advanced solutions, organizations can enhance security practices.

However, organizations must also strengthen organizational factors which are security awareness training, clear policies and procedures, management support for technology budgeting, adherence to protocols, regular incident response communication, collaborative security/IT planning, gathering inputs across units, training for internal expertise, regular risk assessments, and fostering a security-aware culture. Organizational factors like training, policies, management support, communication, collaboration, and a security-focused culture are crucial for enhancing security performance.

Concurrently, organizations align practices with environmental factors such as regulatory requirements, global practices, national strategies, and industry benchmarks to enhance security posture. Specifically, aligning with regulations ensures compliance, adopting global practices promotes interoperability, and benchmarking against industry standards enables continuous improvement. Ultimately, aligning with these environmental factors mitigates risks, fosters stakeholder trust, and contributes to improved organizational performance in information security practices.

5.5 Further Research Implications

Comparative Studies Across Different Sectors, Future research could explore the effect of information security practices on organizational performance in other sectors beyond banking. Moreover, comparative studies across different industries can provide a broader understanding of how information security practices influence performance in various contexts. Additionally, researchers could investigate the unique challenges and requirements of different sectors, such as healthcare, government, or manufacturing, to develop tailored information security strategies.

In addition to comparative studies, qualitative research methods, such as interviews, focus groups, and case studies, can provide valuable insights into the non-quantifiable aspects of security practices, including employee perceptions, organizational culture, and intangible benefits like reputation and customer trust. Furthermore, qualitative data can help organizations understand the human and cultural factors that influence the effectiveness and adoption of security measures, enabling a more comprehensive cost-benefit evaluation.

Moreover, cultural and behavioral aspects of information security within organizations needs further investigation. Specifically, exploring how organizational culture, employee behavior, and psychological factors influence security practices can provide deeper insights into developing more effective security strategies. This includes examining the role of leadership, communication, and employee engagement in fostering a security-conscious culture. Moreover, research could delve into the cognitive biases and decision-making processes that effect security-related behaviors.

Regarding regulatory aspects, research could also examine the implications of national and international policies and regulations on information security practices in Ethiopia. Understanding the regulatory landscape and its effect on organizational behavior can help in formulating better policies and compliance strategies. Furthermore, studies could explore the effectiveness of existing policies and regulations, identify potential gaps, and propose recommendations for improving the legal and regulatory framework to enhance information security practices.

Regarding to the technological advancements, as technology continues to evolve rapidly, future research should focus on the implications of emerging technologies, such as artificial intelligence, cloud computing, and the Internet of Things, on information security practices. Consequently, investigating the potential vulnerabilities and risks associated with these technologies can help organizations stay ahead of cyber threats and develop proactive security measures.

Finally, conducting longitudinal studies can offer valuable insights into the long-term effect of information security practices on organizational performance. By tracking organizations over an extended period, researchers can identify patterns, trends, and evolving challenges, thereby enabling them to develop more robust and sustainable security strategies.

References

Abdu, E., 2022. Financial distress situation of financial sectors in Ethiopia: A review paper. Cogent Econ. Finance 10, 1996020. https://doi.org/10.1080/23322039.2021.1996020

Adebola, B.D., 2014. The determinant of information security practices towards organizational performance in the banking sector evidence from Nigeria (phd). Universiti Utara Malaysia.

Agosa, M.B., n.d. Information security Management Practices and Organizational Goals: a study of Microfinanace Organizations in Nairobi.

Alahmari, A., Duncan, B., 2020. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence, in: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). pp. 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Al-Bassam, S., Al-Alawi, A., 2019. The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector.

Allen, M.W., Brady, R.M., 1997. Total Quality Management, Organizational Commitment, Perceived Organizational Support, and Intraorganizational Communication. Manag. Commun. Q. 10, 316–341. https://doi.org/10.1177/0893318997010003003

Alshaikh, M., n.d. Information Security Management Practices in Organisations.

Alshaikh, M., Maynard, S.B., Ahmad, A., Chang, S., 2018. An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. Hawaii Int. Conf. Syst. Sci. 2018 HICSS-51.

Anderson, C., Baskerville, R.L., Kaul, M., 2017. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. J. Manag. Inf. Syst. 34, 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

Barona, R., Anita, E.A.M., 2017. A survey on data breach challenges in cloud computing security: Issues and threats, in: 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT). Presented at the 2017 International Conference on Circuit ,Power

and Computing Technologies (ICCPCT), pp. 1–8. https://doi.org/10.1109/ICCPCT.2017.8074287

Barras, R., 1990. Interactive innovation in financial and business services: The vanguard of the service revolution. Res. Policy 19, 215–237. https://doi.org/10.1016/0048-7333(90)90037-7

"Bryan" Jean, R., Sinkovics, R.R., Kim, D., 2008. Information technology and organizational performance within international business to business relationships: A review and an integrated conceptual framework. Int. Mark. Rev. 25, 563–583. https://doi.org/10.1108/02651330810904099

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 523–548.

Camillo, M., 2017. Cybersecurity: Risks and management of risks for global banks and financial institutions. J. Risk Manag. Financ. Inst. 10, 196–200.

Cascio, W.F., Montealegre, R., 2016. How Technology Is Changing Work and Organizations. Annu. Rev. Organ. Psychol. Organ. Behav. 3, 349–375. https://doi.org/10.1146/annurev-orgpsych-041015-062352

Chen, C., Shaw, R.-S., Yang, S., 2006. Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. IT Learn. Perform. J. 24.

Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q., 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Comput. Secur. 39, 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F., Materne, S., 2022. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap. Risk Insur. Issues Pract. 47, 698–736. https://doi.org/10.1057/s41288-022-00266-6

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Dutta, A., McCrohan, K., 2002. Management's Role in Information Security in a Cyber Economy. Calif. Manage. Rev. 45, 67–87. https://doi.org/10.2307/41166154

Frangopoulos, E.D., Eloff, M.M., Venter, L.M., n.d. SOCIAL ASPECTS OF INFORMATION SECURITY.

Gebremichael, T., Ledwaba, L.P.I., Eldefrawy, M.H., Hancke, G.P., Pereira, N., Gidlund, M., Akerberg, J., 2020. Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. IEEE Access 8, 152351–152366. https://doi.org/10.1109/ACCESS.2020.3016937

Hassan, M.K., Sanchez, B., Yu, J.-S., 2011. Financial development and economic growth: New evidence from panel data. Q. Rev. Econ. Finance 51, 88–104. https://doi.org/10.1016/j.qref.2010.09.001

Herath, T., Rao, H.R., 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 47, 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hong, K., Chi, Y., Chao, L.R., Tang, J., 2003. An integrated system theory of information security management. Inf. Manag. Comput. Secur. 11, 243–248. https://doi.org/10.1108/09685220310500153

Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. Decis. Sci. 43, 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Huang, K., Wang, X., Wei, W., Madnick, S., 2023. The Devastating Business Impacts of a Cyber Breach. Harv. Bus. Rev.

Kalogiannidis, S., 2021. Impact of employee motivation on organizational performance. A scoping review paper for public sector. Strateg. J. Bus. Change Manag. 8 3 984 996.

Kayworth, T., Whitten, D., 2012. Effective Information Security Requires a Balance of Social and Technology Factors.

Kebebe, E., 2019. Bridging technology adoption gaps in livestock sector in Ethiopia: A innovation system perspective. Technol. Soc. 57, 30–37. https://doi.org/10.1016/j.techsoc.2018.12.002

Kim, K.Y., Eisenberger, R., Baik, K., 2016. Perceived organizational support and affective organizational commitment: Moderating influence of perceived organizational competence. J. Organ. Behav. 37, 558–583. https://doi.org/10.1002/job.2081

Knapp, K.J., Morris, R.F., Marshall, T.E., Byrd, T.A., 2009. Information security policy: An organizational-level process model. Comput. Secur. 28, 493–508. https://doi.org/10.1016/j.cose.2009.07.001

Kong, H., Jung, S., Lee, I., Yeon, S.-J., 2015. Information Security and Organizational Performance: Empirical Study of Korean Securities Industry. ETRI J. 37, 428–437. https://doi.org/10.4218/etrij.15.0114.1042

Kuswati, Y., 2020. The Effect of Motivation on Employee Performance. Bp. Int. Res. Crit. Inst.-J. BIRCI-J. 3, 995–1002. https://doi.org/10.33258/birci.v3i2.928

Lebek, B., Uffen, J., Neumann, M., Hohler, B., H. Breitner, M., 2014. Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. 37, 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lessa, L., Negash, S., Bogale, M., 2019. Building an Information Security Awareness Program for a Bank: Case from Ethiopia.

Levine, R., 1997. Financial Development and Economic Growth: Views and Agenda. J. Econ. Lit. 35, 688–726.

Liang, H., Xue, Y., 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Q. 33, 71–90. https://doi.org/10.2307/20650279

Masa'deh, R., Al-Henzab, J., Tarhini, A., Obeidat, B.Y., 2018. The associations among market orientation, technology orientation, entrepreneurial orientation and organizational performance. Benchmarking Int. J. 25, 3117–3142. https://doi.org/10.1108/BIJ-02-2017-0024

Melville, N., Kraemer, K., Gurbaxani, V., 2004. Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value. MIS Q. 28, 283–322. https://doi.org/10.2307/25148636

Mithas, S., Ramasubbu, N., Sambamurthy, V., 2011. How Information Management Capability Influences Firm Performance. MIS Q. 35, 237–256. https://doi.org/10.2307/23043496

Negussie, A., 2015. Practices, Challenges and Prospects of Informaiton Secuirty Policy in Ethiopian Banking Industry (Thesis). Addis Ababa University.

Nguyen, T.H., Le, X.C., Vu, T.H.L., 2022. An Extended Technology-Organization-Environment (TOE) Framework for Online Retailing Utilization in Digital Transformation: Empirical Evidence from Vietnam. J. Open Innov. Technol. Mark. Complex. 8, 200. https://doi.org/10.3390/joitmc8040200

Nnaeto, J., Juliet Anulika, N., 2018. Impact of Motivation on Employee Performance: A Study of Alvan Ikoku Federal College of Eduaction. J. Manag. Strategy 9, 53. https://doi.org/10.5430/jms.v9n1p53

Pahnila, S., Siponen, M., Mahmood, A., 2007. Employees' Behavior towards IS Security Policy Compliance. pp. 156b–156b. https://doi.org/10.1109/HICSS.2007.206

Pearson, S., 2013. Privacy, Security and Trust in Cloud Computing, in: Pearson, S., Yee, G. (Eds.), Privacy and Security for Cloud Computing, Computer Communications and Networks. Springer, London, pp. 3–42. https://doi.org/10.1007/978-1-4471-4189-1_1

Pérez-González, D., Preciado, S.T., Solana-Gonzalez, P., 2019. Organizational practices as antecedents of the information security management performance: An empirical investigation. Inf. Technol. People 32, 1262–1275. https://doi.org/10.1108/ITP-06-2018-0261

Samonas, S., Coss, D., 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. J. Inf. Syst. Secur. 10.

Schlienger, T., Teufel, S., 2003. Information security culture - from analysis to change : research article. South Afr. Comput. J. 2003, 46–52. https://doi.org/10.10520/EJC27949

Selamat, M., Babatunde, D.A., 2014. Mediating Effect of Information Security Culture on the Relationship between Information Security Activities and Organizational Performance in the Nigerian Banking Setting. Int. J. Bus. Manag. 9. https://doi.org/10.5539/ijbm.v9n7p33

Singh, A.N., Gupta, M.P., 2019. Information Security Management Practices: Case Studies from India. Glob. Bus. Rev. 20, 253–271. https://doi.org/10.1177/0972150917721836

Sohrabi Safa, N., Von Solms, R., Furnell, S., 2016. Information security policy compliance model in organizations. Comput. Secur. 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Soomro, Z.A., Shah, M.H., Ahmed, J., 2016. Information security management needs more holistic approach: A literature review. Int. J. Inf. Manag. 36, 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Tanrıverdi, N., Metin, B., 2021. Enterprise Information Security Awareness and Behavior as an Element of Security Culture During Remote Work. pp. 119–138. https://doi.org/10.4018/978-1-7998-7513-0.ch008

Thakur, H., 2021. Research Design. p. 175.

Ullah, A., Iqbal, S., Shams, S.M.R., 2020. Impact of CRM adoption on organizational performance. Compet. Rev. Int. Bus. J. 30, 59–77. https://doi.org/10.1108/CR-11-2019-0128

Urbinati, A., Chiaroni, D., Chiesa, V., Frattini, F., 2020. The role of digital technologies in open innovation processes: an exploratory multiple case study analysis. RD Manag. 50, 136–160. https://doi.org/10.1111/radm.12313

Vacca, J.R., 2012. Computer and Information Security Handbook. Newnes.

Viegas, V., Kuyucu, O., 2022. International Security Standards, in: IT Security Controls: A Guide to Corporate Standards and Frameworks. Apress, Berkeley, CA, pp. 17–65. https://doi.org/10.1007/978-1-4842-7799-7_2

von Solms, R., 1999. Information security management: why standards are important. Inf. Manag. Comput. Secur. 7, 50–58. https://doi.org/10.1108/09685229910255223

von Solms, R., van Niekerk, J., 2013. From information security to cyber security. Comput. Secur., Cybercrime in the Digital Economy 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Yunis, M., Tarhini, A., Kassar, A., 2018. The role of ICT and innovation in enhancing organizational performance: The catalysing effect of corporate entrepreneurship. J. Bus. Res. 88, 344–356. https://doi.org/10.1016/j.jbusres.2017.12.030

APPENDICES

ADDIS ABABA UNVERSITY

COLLEGE OF BUSINESS AND ECONOMICS SCHOOL OF COMMERCE

DEPARTMENT OF BUSINESS ADMINISTRATION AND INFORMATION SYSTEMS

Research Questionnaire

Dear respondent,

I am a student at Addis Ababa University's graduate school, conducting research on "Information security practices towards organizational performance in private banks of Ethiopia". The purpose of this study is to assess how certain information security practices influence the performance of private banks. Your time and candid feedback are greatly appreciated, as they will provide valuable insights on this important topic.

Please note:

• Your participation is voluntary, and you are not required to provide your name.

• All responses will be kept strictly confidential and used only for academic purposes.

• Please mark ✓ in the boxes available for your responses.

If you have queries regarding to questionnaire, you can reach me using the following number +251936979200 and email address wondiyenahom@gmail.com

Thank you

Yours faithfully,

Nahom Wondiye

SECTION A: Background Information

Here general questions regarding the participant's profile are given. Please indicate your choice by marking (✓) against your choice.

1. Gender

   ☐ Female ☐ Male

2. Age

   ☐ 18-25 ☐ 26-35

   ☐ 36-44 ☐ 45 & above

3. Highest educational level obtained:

   ☐ Diploma ☐ MA/MSc

   ☐ BA/BSC Degree ☐ Other

4. Work Experience in the Financial Industry (in years):

   ☐ 1-3 ☐ 7-9

   ☐ 4-6 ☐ 10-13 ☐ Above 14

5. Have you ever taken any type of training on information security?

   ☐ Yes ☐ NO

6. Do you have any certificate regarding to information security?

   ☐ Yes ☐ NO

SECTION B: Technological, Organizational, environmental factors

The aim of this section is to explore your opinion technological, organizational, environmental factors towards organizational performance.

Please answer the following questions using this 5-points scale.

1 = Strongly Disagree *2 = Disagree* *3 = Neither agree nor disagree* *4 = Agree* *5 = Strongly Agree*

Technological Factors towards organizational performance						
S. No.	**Items**	**1**	**2**	**3**	**4**	**5**
1	your existing IT infrastructure supports secure and compliant business operations.					
2	The technical skills of your IT staff and capabilities of your technologies equip the organization to prevent, detect and respond to security threats.					
3	The level of integration and collaboration between technology and security teams strengthen security defenses and performance.					
4	Investment in new security technologies improves organizational performance.					
5	The bank's technological readiness enables secure digital services.					
Organizational factors toward organizational performance						
S. No.	**Items**	**1**	**2**	**3**	**4**	**5**
6	Security awareness training improves employee technical skills and ability to support secure organizational operations.					
7	Clear security policies and procedures streamline technology governance and compliance with requirements.					
8	Management commitment to technology budgeting optimizes controls and infrastructure defending critical systems.					
9	Adherence to information security policies and protocols as part of employee performance evaluations contributes to more secure and productive use of technology by staff.					
10	Regular communication of established security incident response procedures improves information security awareness and preparedness across the organization.					
11	Involving security and IT teams in collaborative planning and policy development encourages buy-in and shared accountability for maintaining information security standards					
12	Gathering inputs from all business units helps drive management commitment to align security spending with strategic needs and operational requirements.					

13	Providing training and resources to build internal security expertise ensures policies and technologies are properly implemented and managed throughout the organization					
14	Conducting regular risk assessments and sharing results helps update security protocols to address emerging threats to business operations.					
15	Promoting a security-aware culture fosters cross-team collaborations that strengthen implementation of measures protecting sensitive data and systems.					
Environmental factors towards organizational performance						
S. No.	**Items**	**1**	**2**	**3**	**4**	**5**
16	Regulatory certification requirements for security systems and practices improve technical controls, governance and incident response supporting secure operations.					
17	Alignment with global security practices through regional cooperation strengthens protection of critical data and infrastructure defending the organization.					
18	Adherence to national security strategies harmonizes technical defenses and roles/processes benefiting compliant operations.					
19	Benchmarking security controls, access management and platform resilience with peers in the Ethiopian banking sector fuels continuous improvement.					
Organizational Performance						
20	The implementation of new technology has positively impacted the performance of the organization.					
21	The organizational structure and processes significantly contribute to the performance of the organization.					
22	External factors have a significant influence on the performance of the organization.					

THANK YOU FOR YOUR COOPERATION!!