ST. MARY'S UNIVERSITY

SCHOOL OF BUSINESS

THE EFFECTS OF CYBER-ATTACKS ON BANKS BUSINESS ICT SYSTEMS: THE CASE OF BANKS IN ETHIOPIA

By: BISRAT AIMERO

JUNE 2023

ADDIS ABABA, ETHIOPIA

THE EFFECTS OF CYBER-ATTACKS ON BANKS BUSINESS ICT SYSTEMS: THE CASE OF BANKS IN ETHIOPIA

BY: BISRAT AIMERO

ID NO. SGS/0033/2013B

A THESIS SUBMITTED TO ST. MARY'S UNIVERSITY, SCHOOL OF GRADUATE STUDIES FOR PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION

ADVISOR: TEWODROS MEKONNEN (PhD)

ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

BOARD OF EXAMINERS

THE EFFECTS OF CYBER-ATTACKS ON BANKS BUSINESS ICT SYSTEMS: THE CASE OF BANKS IN ETHIOPIA

As members of the Examining Board of the final MBA open defense, we certify that we read and evaluated the thesis prepared by Bisrat Aimero Taddesse and recommend that it be accepted as fulfilling the thesis requirement for the Degree of Master of Business Administration.

_____	_____
Name of Chairman	Signature and Date
_____	_____
Name of Advisor	Signature and Date
_____	_____
Name of External Examiner	Signature and Date
_____	_____
Name of Internal Examiner	Signature and Date

DECLARATION

I declare that this thesis entitled “The effects of cyber-attacks on banks business ICT systems: The case of banks in Ethiopia” is my original work, and has never been presented for the award of any degree in this or any other university and all sources of materials used for the thesis have been duly acknowledged.

Name: Bisrat Aimero

Signature _____

Date _____

June 2023
Addis Ababa, Ethiopia

ENDORSEMENT

I confirm that this work entitled “The effects of cyber-attacks on banks business ICT systems: The case of banks in Ethiopia” is the original work of Bisrat Aimero. Hence, I recommend the submission of the thesis to St. Mary’s University, School of Graduate Studies for examination with my approval as a university advisor.

Advisor's Name: Tewodros Mekonnen (Ph.D.)

Signature _____

Date _____

ACKNOWLEDGEMENT

Initially, I offer my immeasurable gratitude to the Almighty God and His Mother Saint Mary for bestowing upon me the opportunities, abilities, and guidance that have shaped my life. Next, I would like to express my sincere gratitude to all those who have supported me throughout the process of completing this thesis.

First and foremost, I would like to extend my heartfelt appreciation to my advisor, Dr. Tewodros Mekonnen (Ph.D.), for their guidance, expertise, and unwavering support. His invaluable insights, constructive feedback, and continuous encouragement have been instrumental in shaping this research.

I am indebted to my family (Alazar, Elizabeth, Misrak, Tsegereda, and Temesgen) for their unwavering support, love, and encouragement. I also would like to thank my friends (Zewdu and Nakachew) for their endless support until the end with advice and materials. Their belief in me and their understanding during challenging times have been a constant source of motivation.

Finally, I would like to thank all the participants who generously devoted their time and contributed to the data collection process, to authors, researchers, and scholars whose work I have referenced played vital roles in this thesis. I acknowledge their significant impact on this endeavor is truly appreciated.

Table of content

Contents

List of Tables

List of Figures

List of Abbreviations

Abbreviation	*Definition*
ATM	Automated Teller Machine
BI	Business Intelligence
CERT	Cyber Emergency and Response Team
CFO	Chief Financial Officer
CIA	Confidentiality Integrity and Availability
CMCSRS	Critical Mass Cyber Security Requirement Standard
COA	Compromise of Availability
COC	Compromise of Confidentiality
COI	Compromise of Integrity
CSAF	Cyber Security Auditing Framework
CSO	Chief Security officer
DDOS	Distributed Denial of Service
FIS	Financial Intelligence Service
IBM	International Business Machine
ICT	Information Communication Technology
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
INSA	Information Network Security Administration
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
ITU	International Telecommunication Union
MFI	Micro Finance Institutions
NBE	National Bank of Ethiopia
NEFT	National Electronic Fund Transfer
NIST	National Institute of Standards and Technology
POS	Point of Sale
RTGS	Real Time Gross Settlement
SME	Small and Medium Enterprises
SOC	Security Operation Center
SPSS	Statistical Package for Social Science
SQL	Structured Quarry Language
UNGGE	United Nations Group of Governmental Experts
UPI	Unified Payment Interface
XSS	Cross-Site Scripting

ABSTRACT

This study examines the effect of cyber-attacks on Ethiopian banks' ICT systems and explores the fundamental mechanisms for protecting against these attacks. In this, an explanatory research design within the framework of a mixed-method research approach, combining qualitative and quantitative methods, was employed to frame the research and gather comprehensive data. Both primary and secondary data are used in the study. A Census strategy is followed to gather data from banks' headquarters found in the country. Quantitative and qualitative methods of data analysis are used to give meaning to the raw data. The findings of the study indicate that malware, DDOS, and fishing attacks are the most commonly observed cyber-attacks on banks' ICT systems. Most importantly, all of the explanatory variables (Compromise of confidentiality, integrity, and availability) significantly affect the bank's ICT systems negatively. In general, the study provided valuable understanding into common types of cyber-attacks faced by Ethiopian banks, cybersecurity measures implemented, effect on ICT systems, vulnerability management, detection and response capabilities, and collaboration efforts with stakeholders. As a recommendation, the findings highlight the need for proactive cybersecurity strategies, multi-layered security controls, regular vulnerability assessments, and incident response planning.

Key Words: Cyber-attacks, Banks' ICT systems, Confidentiality, Integrity, Availability

Chapter One

Introduction

1.1. Background of the study

Information and Communication Technology (ICT) is a broad term that encompasses a wide range of technologies used for the processing, storage, and communication of information (International Telecommunication Union [ITU], 2023). These technologies have transformed how we live and work, enabling us to communicate instantly, access vast amounts of information, and automate many tasks. ICT has played a crucial role in the technological revolution, facilitating the transition from traditional to modern forms of communication, and has enabled businesses to expand and become more productive. With the rise of ICT, traditional industries such as finance systems have been transformed, with many companies now relying on digital technologies to manage operations and reach customers (Triki & Faye, 2013).

Cyber refers to the virtual world of computers, networks, and digital information (Diogenes & Ozkaya, 2018). Cybersecurity is the practice of protecting computer systems, networks, and digital information from unauthorized access, theft, damage, and other cyber threats (Li, 2017). It involves implementing security measures such as firewalls, antivirus software, and encryption to safeguard sensitive data and prevent cyber-attacks. A cyber-attack is any malicious attempt to disrupt, damage, or gain unauthorized access to a computer system or network. These attacks can take many forms, including malware infections, phishing scams, and denial-of-service attacks (Debra L, 2002). As our reliance on digital technologies grows, the threat of cyber-attacks also increases, and the financial sector is particularly vulnerable to such attacks due to its heavy reliance on digital technologies for transactions, data storage, and communication (Cambridge, 2017). In Ethiopia, as in many developing countries, the financial sector is rapidly expanding and modernizing, making it an essential area of study for understanding the effects of cyber attacks on this sector.

Financial institutions are corporations that provide services as intermediaries of financial markets (Tariq, 2018). A financial institution is responsible for the supply of money to the market through

the transfer of funds from investors to the companies in the form of loans, deposits, and investments (Tariq, 2018).

The Ethiopian financial sector is one of the fastest developing sectors in the country, with the establishment of new financial organizations such as commercial banks and Micro-Finance Institutions. According to the National Bank of Ethiopia, the country's financial sector has been growing at an average annual rate of 25% in recent years, with the number of commercial banks increasing from 4 in 1994 to over 40 by 2021(NBE, 2021) In addition to commercial banks, the country has also seen the establishment of Micro-Finance Institutions (MFIs), which play an essential role in providing financial services to the unbanked population in rural areas. As of 2020, 34 licensed MFIs were operating in Ethiopia, serving over 5 million clients with a total loan portfolio of over 21 billion Ethiopian Birr(Global Microscope, 2020).

Banks are still the dominant participants and contributors in the financial sector; as such financial institutions are engines of growth and transformation in the nation. Financial sector development has played a vital role in Ethiopia's economic development (Birru, 2019) Yet most of these infrastructures and company facilities nowadays rely on computer systems almost daily. With the advances in information technology, most banks in Ethiopia have migrated to core banking platforms and moved transactions to payment cards (visa cards) and to electronic channels like ATMs, growing aggressively at an alarming rate. Fintech, or financial technology, refers to the use of technology to improve and automate financial services, including banking, insurance, and investment management (Bezabeh, 2015). Mobile money services have gained popularity in Ethiopia, with platforms like M-Birr, Amole, and Hello Cash enabling people to send and receive money, pay bills, and make transactions using their mobile phones (Lessa & Negash, 2019). In this regard, the concept of banking technology is related to the expansion of the Internet and other information communication innovated devices (Woretaw & Lessa, 2012).

According to(Asfaw et al., 2018), the rapid development and adoption of information and communication technology (ICT) in the financial sector have made it vulnerable to cyber-attack from potential threat agents such as threat agents like cyber fraudsters, cybercriminals, hackers, attackers, terrorist groups, insider attackers, enemy countries, and other motivated individuals or groups. (Debra L, 2002) defines cybercrime as any criminal offense committed using the internet or another computer network as a component of the crime. Cybercrimes are offenses committed

against individuals or groups of individuals with a criminal motive to internationally harm the victim's reputation or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as the internet and mobile phones. Such crimes may threaten the nation's security and financial health. (PWC, 2014).

Additionally, the lack of awareness and training of employees in the financial sector regarding cyber threats has made it easier for hackers to penetrate the system (Abraha & Hailu, 2015). Furthermore, the limited regulatory framework and absence of clear guidelines on cybersecurity in Ethiopia have created gaps that hackers can exploit (Lessa & Negash, 2019). The financial sector, including banks, is vulnerable to cyber threats due to several factors, such as inadequate cybersecurity infrastructure, weak passwords, phishing attacks, insider threats, and third-party risks (Gerami, 2018).

This research paper aims to present the effects of cyber-attacks on Ethiopia's financial sectors, especially the banking sector. Even though there is inadequate research conducted on the area, the study tried to identify the type of cyber-attacks, the attacker's motive, and their effects on the business or how much damage had been done to the financial sector. The study utilized data from the Information Network Security Administration over the past few years, and the study had also use expertise from the field of cyber security. The study addressed which type of cyber-attacks pose a risk to the financial sector and how much they affect the financial system.

1.2. Statement of the problem

Technology has integrated nations, and the world has become a global village. The technologies used by the financial industries are accessible and open to everybody. However, the information technology revolution associated with the internet has brought about two edge functions: on the one hand, it has contributed positive values to the world. While on the other hand, it has produced so many maladies that threaten the order of society and also produce a new wave of crime in the world. The advancement of technology has transformed the banking sector, facilitated seamless operations, and delivered more efficient services. However, as technology evolves, so do the risks associated with it. Cyber-attacks, in particular, have emerged as a significant threat to the banking industry, causing unprecedented damage to banks and their customers (Li, 2017).

Define cybercrime (Debra Shinder, 2002), as any criminal offense committed using the internet or another computer network as a component of the crime. Cybercrimes are offenses committed against individuals or groups of individuals with a criminal motive to internationally harm the victim's reputation or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as the internet and mobile phones. Such crimes may threaten the nation's security and financial health (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018).

The financial losses from cyber-attacks on banks have increased in recent years (Manivannan & Moorthy, 2020). In addition to the direct financial losses, cyber-attacks also cause reputational damage to banks, negatively affecting customer trust and loyalty (Triki & Faye, 2013b). Cyber-attacks' effect on banks has been studied extensively, with researchers emphasizing the need to develop and implement effective cybersecurity measures to mitigate the associated risks (Bouveret et al., 2018).

The theoretical linkage between cyber-attacks and the Confidentiality, Integrity, and Availability of financial systems is based on the fundamental principles of information security. Confidentiality refers to protecting sensitive information from unauthorized disclosure or access, and integrity refers to protecting information from unauthorized modification or destruction, ensuring that it remains accurate and complete. Availability refers to the accessibility of information and services to authorized users when needed (NIST, 2021.).

Cyber-attacks can compromise the Confidentiality, Integrity, and Availability of financial systems in various ways. For instance, hackers can gain unauthorized access to confidential financial information, such as customer data, transaction records, and account details, through attacking methods like phishing, social engineering, or malware attacks. This can lead to identity theft, financial fraud, and reputational damage to financial institutions. Similarly, cyber-attacks can also compromise the Integrity of financial systems by tampering with or modifying financial data, such as altering transaction records, account balances, or stock prices, leading to financial losses or market disruptions. Finally, cyber-attacks can also affect the Availability of financial systems by disrupting or disabling critical services, such as online banking, payment systems, or stock exchanges, leading to business interruptions and financial losses. ('The CIA triad: Definition, components, and examples | CSO Online,' n.d.).

Global Studies:

Numerous studies have investigated the impact of cyber-attacks on banks globally. For example, (PWC, 2014) conducted a comprehensive review of the literature on cybersecurity and the financial sector and found that cyber-attacks significantly impact banks' financial performance. Similarly, (Stanikzai & Shah, 2021)studied the impact of cyber-attacks on bank stock prices and found that cyber incidents had a negative effect on stock prices, leading to significant financial losses for banks. In addition, Agrafiotis and Nurse (Agrafiotis et al., 2018) conducted a systematic review of cybersecurity threats in the financial sector and found that cyber-attacks significantly threatened the stability and resilience of financial systems globally. Similarly, (Raghavan, 2014) and (Brogi, Arcuri, & Gandolfi, 2018)investigated the effect of cybersecurity on the financial performance of banks in Pakistan and found that cyber-attacks led to significant financial losses and reputational damage for banks.

African Studies:

Studies have also investigated the effect of cyber-attacks on banks in Africa. For example, Okeshola and Adeta (Okeshola & Adeta, 2013) studied the effect of cybersecurity on banking in Nigeria and found that cyber-attacks had a significant effect on the financial performance of banks, leading to significant financial losses and reputational damage. Similarly, Kwadade-Cudjoe et al. Bunmi A (Kwadade-Cudjoe, Enoch, & Bunmi, 2019) investigated the effect of cyber-attacks on network operations in Ghana and found that cyber incidents significantly affected the Confidentiality, Integrity, and Availability of financial systems, leading to financial losses and reputational damage.

Ethiopian Studies:

There are limited studies that have investigated cyber-attack issues and their effect on banks in Ethiopia. Even though there are few studies on the issues, the focus of their studies is more on frameworks, policy, and cyber law-related aspects. However, a study by Tesfaye Asefaw (Asfaw et al., 2018) investigated the cybersecurity auditing frameworks of banks in Ethiopia and found that most banks lacked adequate cybersecurity measures to protect critical assets, leading them to be vulnerable to cyber-attacks. Another study by Abiy and Lemma (2018) and (Woretaw & Lessa 2012)investigated information security culture in the banking sector in Ethiopia and found that information security awareness in the sector is unsatisfactory.

In summary, the above reviews of studies on "the impact of cyber-attacks on banks" globally and in Africa show that cyber-attacks significantly impact banks' financial performance and stability. Nevertheless, in the Ethiopian context, there is a lack of comprehensive data on the type, frequency, nature, and severity of cyber-attacks on banks in Ethiopia. These banks do not have a full-scale awareness of the level of vulnerability to cyber-attacks. Hence this may result in a crisis in the future. This is an issue that needs intervention and needed to be addressed. Therefore, if the research is conducted and shows the problems the sector and others will benefit from its findings. Due to this, the researcher decided to study the matter. Moreover, there is limited research on the effect of cyber-attack on banks in Ethiopia.

Given the above facts, it is implied that a study on how the financial sector is affected due to the risk of cyber-attacks needs to be explored. Overall, more research is needed to address these gaps and provide a better understanding of the effect of cyber-attacks on banks in Ethiopia. This research undertook global demographics in the Ethiopian context, where financial institutions became cyber-attack victims. This study presented an overall view and effect of cyberattacks on financial institutions, and this research is very significant for emerging financial institutions and industry leaders.

1.3. Research questions

The study was directed by the following research questions to address the research problem

1. What are the common types of cyber-attacks that target banks' business ICT systems?
2. How does compromise of confidentiality affect a bank’s business ICT systems?
3. What are the effects of compromise of integrity on a bank's business ICT systems?
4. What is the influence of compromise of availability on a bank’s business ICT system?

4.1. Research objectives

4.1.1. General objective

The general objective of the research is to examine the effects of cyber-attacks on banks business ICT systems in Ethiopia.

4.1.2. Specific objectives

1. To identify the common cyber-attack types that target banks' business ICT systems.
2. To examine the effect compromise of confidentiality on banks' business ICT systems.
3. To examine the effect compromise of integrity on banks' business ICT systems.
4. To examine the effect compromise of availability on banks' business ICT systems.

4.2. Significance of the study

The significance of this study lies in its potential to identify the common types of cyber-attacks on critical systems of banks and understand their effects. The research provided insights into what mechanisms banks can use to protect against cyber-attacks and mitigate the associated risks.

The first beneficiary of this research is the banking sector. Cyber-attacks have become a significant threat to the financial industry, as they can compromise the Confidentiality, Integrity, and Availability of critical systems and data and can lead to significant financial losses and reputational damage. As the use of digital technologies and the dependence on online services continue to increase, the risk of cyber-attacks is expected to grow. Banks will be able to use this research to develop effective cybersecurity strategies to prevent, detect, and respond to these threats.

Secondly, the research is significant to cyber security organizations that are responsible to develop regulations and policies at a national level. It will serve as input by showing the current cyber security landscape of the banking sector's people and technology and process. Moreover, the study can inform the policy-making and regulatory efforts related to cybersecurity in the cybersecurity and financial industry and contribute to the broader understanding of the challenges and opportunities associated with cybersecurity in the digital age.

Thirdly, since this is an under-researched area of study in Ethiopia, it will contribute to the cyber security discourse by investigating the common types of cyber-attacks that target banks, their effect on the operations of banks, and the fundamental mechanisms that banks can use to protect against cyber-attacks, this study can contribute to the existing literature on cybersecurity and financial risk management. The study's findings can inform the development of best practices for designing and implementing effective cybersecurity strategies for banks and can guide banks in

enhancing their cybersecurity posture and resilience. At last, the research also helped the researcher to add up the knowledge and skill for doing research.

Overall, this study is significant in its potential to contribute to the advancement of knowledge and practice in the field of cybersecurity and financial risk management and in its potential to inform the decision-making processes of banks, regulators, and other stakeholders in both public and private, as well as to government bodies.

4.3. The scope of the study

The scope of this study is to examine the effect of cyber-attacks on banks in Ethiopia, focusing on the Confidentiality, Integrity, and Availability of banks' business-critical systems. The study was conducted on a sample from various bank headquarters both government and private sectors in Ethiopia, as well as the national cert divisions, and the security teams from the information network security administration (INSA).

Conceptually the research focuses on include identifying the common types of cyber-attacks targeting banks, assessing the effect of cyber-attacks on the operations of banks, and identifying fundamental mechanisms that banks can use to protect against cyber-attacks. In order to do this, the research relies on evaluating the three security pillars (triads) namely confidentiality, integrity, and availability that serve as the industry standard in the field.

Data were collected through surveys, interviews, and document analysis using an explanatory mixed method. This will allow Once the quantitative phase is complete, the researcher then follows up with a qualitative phase to delve deeper into the phenomenon under study. The two phases are interconnected, with the qualitative data helping to explain and interpret the quantitative results.

4.4. Limitations of the study

Despite the importance and relevance of the research topic, this study has some issues and limitations that need to be considered. First, the study relies on secondary data sources and

academic literature, and industry reports (CERT and cyber security auditing teams), which may be subject to bias or limitations in their scope and coverage.

In addition, there is expected to be a "data gap" or "missing data" because most CEOs, CFOs, CSOs, and professionals believe admitting and reporting a cyber incident has damaged their reputation, credibility, and brand image. As a national security organization, teams from national cert and security auditing areas tended to prohibit specific data or sample collection for security reasons. The researcher tried to tackle these issues by trying to get triangulated information as much as possible, the work environment of the researcher also gave a unique opportunity to get some information that is vital for the study.

The other limitation of this study is the small sample size from banks headquarters, national CERT, and security auditing teams, which may limit the generalizability of the findings to other sectors (Even though the contagion model assumes cyber-attack has a probability to affect one or several firms, (Bouveret et al., 2018). To address this limitation, purposive sampling techniques ensured a diverse and representative sample of experts from CERT, security auditing teams, and banks. Other data sources and methods, such as document analysis and expert interviews, supplemented the findings and provided a more comprehensive understanding of the research problem.

While the mentioned issues may pose some limitations, this study is significant in its contribution to understanding cyber resilience in the banking sector. The rigorous research design and methodology ensure the findings' validity and reliability.

4.5. Operational definition

1. Business ICT systems: Business ICT systems, in the context of this thesis, encompass the technological infrastructure, software applications, and communication networks utilized by banks to support their operational processes, including transaction processing, data storage, customer management, and internal communications (Paul Bocij; Andrew Greasley; Simon Hickie, 2020).
2. Cybersecurity triads: The cybersecurity triads refer to the three fundamental principles of information security, namely confidentiality, integrity, and availability. Confidentiality involves protecting sensitive information from unauthorized access or disclosure. Integrity ensures the accuracy and reliability of data, preventing unauthorized alterations.

Availability refers to the accessibility and reliability of ICT systems for authorized users. (‘The CIA triad: Definition, components, and examples | CSO Online’, n.d.)

3. Compromise of confidentiality: Compromise of confidentiality refers to the unauthorized disclosure or exposure of sensitive and confidential information, such as customer data, financial records, or trade secrets, which can potentially harm the bank's reputation, violate privacy regulations, and lead to financial losses (Von Solms & Von Solms, 2009).
4. Compromise of integrity: Compromise of integrity refers to unauthorized modifications, alterations, or tampering of data or systems, leading to the loss of data accuracy, reliability, or trustworthiness. This can result in financial inaccuracies, fraudulent activities, or disruptions to critical business operations.(Von Solms & Von Solms, 2009)
5. Compromise of availability: Compromise of availability refers to incidents that result in the unavailability or disruption of the bank's ICT systems, rendering them inaccessible or non-functional. Such incidents may include network outages, server failures, or DDoS attacks, which can impact customer service, transaction processing, and overall business continuity.(Von Solms & Von Solms, 2009)
6. Cyber (Cyberspace): The interconnected network of digital devices, systems, and platforms comprising the internet and other computer networks.(Friis & Ringsmose, n.d.)
7. ICT (Information and Communication Technology): The technology and systems used to process, store, and communicate information, including hardware, software, and telecommunications. (Paul Bocij; Andrew Greasley; Simon Hickie, 2020)
8. Financial sectors: The industries and organizations that are involved in the creation, management, and distribution of financial products and services, including banks, investment firms, insurance companies, and other financial institutions. (Triki & Faye, 2013b)
9. Cyber-attack: A deliberate attempt to compromise the Confidentiality, Integrity, or Availability of a computer system or network using methods such as malware, phishing, or denial of service attacks.(Agrafiotis et al., 2018)
10. Hack꞉- Hacking is identifying security flaws in a computer system or network to gain access to personal data, business data, or organizational data. (Debra L, 2002)

11. Cyber risk: The potential for harm or loss resulting from a cyber-attack or other cyber incidents, including financial losses, reputational damage, and legal liability. (Douglas W. Hubbard, 2016)
12. National CERT team: A national computer emergency response team responsible for responding to cyber incidents and providing advice and guidance to organizations and individuals on how to protect against cyber threats. (Temesgen, 2022)
13. Threat: any potential danger or harm that could exploit a vulnerability in an organization's ICT systems or networks, including malware, phishing, hacking, and social engineering. (PWC, 2014)
14. Malware: Malicious software designed to infiltrate or damage computer systems or networks, such as viruses, Trojans, and ransomware. (Debra L, 2002)
15. Phishing: A social engineering technique used to trick individuals into divulging sensitive information or clicking on malicious links, typically through email or other online communication channels. (Debra L, 2002)
16. DDoS (Distributed Denial of Service): A cyber-attack that overwhelms a computer system or network with traffic, making it unavailable to legitimate users. (Debra L, 2002)

4.6. Organization of the Study

The study is organized into five chapters. Chapter One provides an introduction to the study and presents an overview of the research. Chapter Two focuses on the literature review, where theoretical background and related studies are discussed. In Chapter Three, the research methodology is described, including the research approach, design, and data collection methods. Chapter Four presents the data analysis and presentation of the research findings. Finally, Chapter Five provides a summary of the major findings, conclusions drawn from the study, and recommendations for further action. The study also includes a list of references and annexes related to the research.

Chapter Two

Review of related literature

5.1. Review of theoretical literature

5.1.1. Cyberspace and cyber security

Cyberspace

Cyber and cyberspace generally refer to the virtual world of computing and online communication. Cyberspace is a term used to describe the electronic medium that facilitates online communication and represents a global domain within the information environment consisting of the interdependent network of information systems infrastructures, including the Internet computer networks and other telecommunication networks. (Information Technology Laboratory, Computer Security Resource Center, & Cyberspace, n.d.) In short, cyber and cyberspace refer to the sphere of computers, networks, and online communication and the infrastructure that connects them. It is a term used to describe the virtual world of computing in which we interact over the internet, online platforms, and other forms of electronic communication.

In its financial service report, the Global economic crime and fraud survey describes cyberspace as the fourth domain, after land, sea, and air, where military and civilian activities occur. In the modern world, cyber-attacks have become one of the most significant security challenges, as the internet has enabled actors to conduct attacks on an unprecedented scale and scope. Cyberspace is a complex and interconnected domain with various networks, systems, and devices. Attackers can exploit vulnerabilities in these systems and networks to gain unauthorized access, steal sensitive information, or disrupt critical services. Moreover, cyber-attacks can be launched from anywhere worldwide, making it difficult to attribute them to a specific actor. According to ('Economic Cost of Cybersecurity,' 2020), financial institutions are one of the most targeted sectors, with the average cost of a cyber-attack on a bank being $18.3 million. As the reliance on technology and digital systems continues to increase, the effect of cyber-attacks is likely to become more severe, underscoring the need for effective cybersecurity measures to protect against cyber threats.

Cyberattacks and the banking sector have been a topic of great interest to researchers due to the significant effect that cyberattacks can have on the Confidentiality, Integrity, and Availability of

banking data. Cyberattacks are defined as any malicious attempt to compromise the security of information systems, devices, or networks. According to (Manivannan & Moorthy, 2020) cyberattacks can be categorized into four main types: passive, active, insider, and outsider attacks.

Cyber Security

Cybersecurity protects electronic devices, networks, and sensitive data from unauthorized access, theft, and damage. The term encompasses a range of security measures and protocols designed to ensure the Confidentiality, Integrity, and Availability of digital assets.

Cybersecurity has become a critical issue for businesses and governments worldwide due to the increasing frequency and severity of cyber-attacks. The World Economic Forum has identified cyber-attacks as one of society's top global risks('These are the top cybersecurity challenges of 2021 | World Economic Forum', n.d.) A cyber-attack deliberately exploits computer systems, networks, and devices to cause harm, theft, or disruption. Cyber-attacks can take various forms, including malware, phishing, hacking, ransomware, and distributed denial-of-service (DDoS) attacks (Diogenes & Ozkaya, 2018). These attacks can have severe consequences, ranging from financial losses to reputational damage and physical harm. Therefore, cybersecurity is a critical concern for organizations and governments, requiring constant attention and investment in prevention and response measures.

One of the critical challenges in cybersecurity is the dynamic nature of cyber threats. Attackers continuously evolve their tactics and techniques to evade detection and exploit vulnerabilities in systems and networks. Therefore, adopting a proactive and adaptive approach to cybersecurity is essential to incorporate risk management, threat intelligence, and incident response ('Simple Overview of CMMC and NIST 800-171: Ready, Set, go!', n.d.) Additionally, cybersecurity requires collaboration and coordination between various stakeholders, including government agencies, private sector organizations, and individual users. The development of international norms and standards, such as the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), can help promote cooperation and build trust among nations(UN, 2023) Overall, the literature highlights the importance of cybersecurity in modern society and the need for a holistic and collaborative approach to address the evolving cyber threat landscape.

5.1.2. Theoretical models of cyber attack

Frameworks such as the CIA triad model, cyber kill chain model, and diamond model have been developed to understand the theoretical linkage between various entities in cyber security.

1. The CIA triad model

The CIA triad model describes three critical components of information security: Confidentiality, Integrity, and Availability. Confidentiality refers to protecting sensitive information from unauthorized access, Integrity refers to ensuring the accuracy and completeness of information, and Availability refers to ensuring that authorized users have access to information when needed (NIST, 2021)

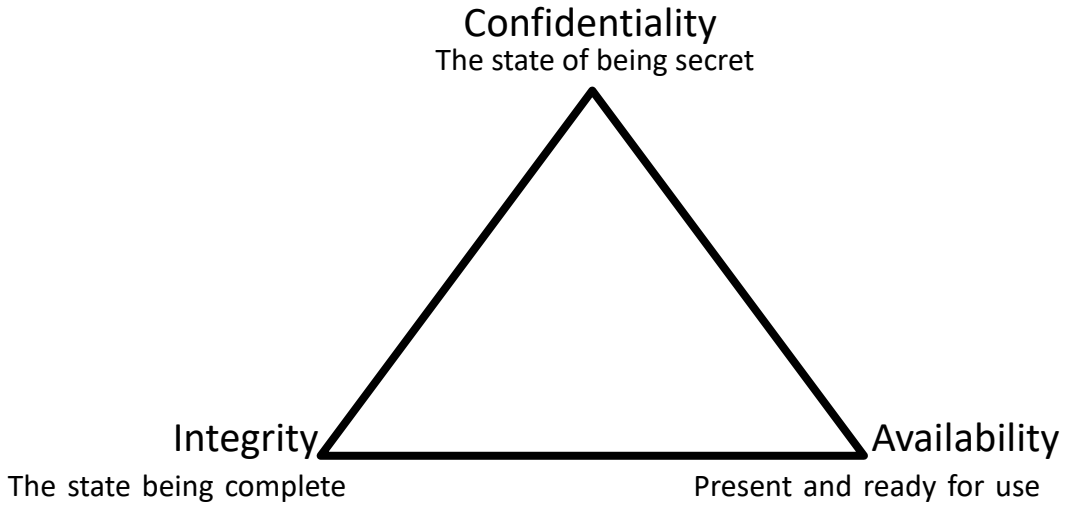

Figure 1: The CIA Triad Model

Source:(NIST SP: 80053)

On the other hand, the attack tree model is used to analyze the steps involved in a cyberattack and identify potential vulnerabilities in the system. The model is based on the idea that an attacker must first identify vulnerabilities in the system, then exploit those vulnerabilities to gain access, and finally take control of the system (Kott, Lange, & Ludwig, 2018).

2. The cyber kill chain model

As described in the book Cybersecurity – Attack and Defense Strategies (Diogenes & Ozkaya, 2018), There is no standard or universally accepted set of steps for hacking, as different hackers and security experts may use different methods and frameworks. However, one commonly used

framework is the "Kill Chain" model, which consists of 7 stages The cyber-attack process involves several stages. It begins with reconnaissance, where the attacker gathers information about the target system, including its network structure, configurations, vulnerabilities, and potential ways to launch an attack. Once the weaknesses are identified, the attacker proceeds to weaponization by creating or obtaining tools and malware specifically designed to exploit those vulnerabilities.

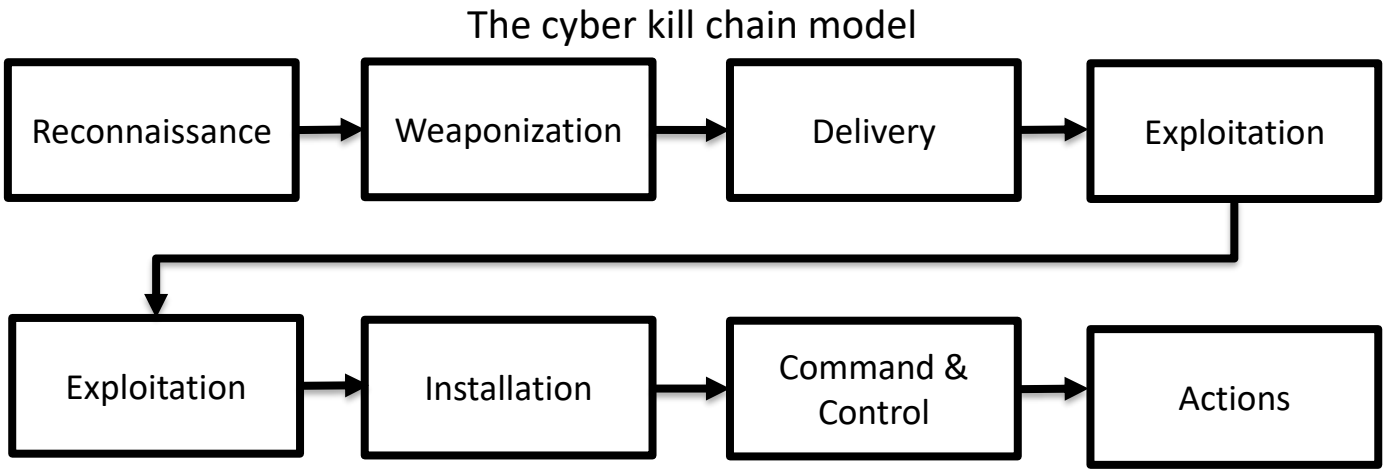

Figure 2: The Cyber Kill Chain Model

Source: (Diogenes & Ozkaya, 2018),

The weaponized payload is then delivered to the target system through various means, such as email attachments, social engineering techniques, or exploiting weaknesses in websites. Once delivered, the payload is executed on the target system, taking advantage of vulnerabilities, weak passwords, or misconfigured access controls to gain unauthorized access or control. The attacker may also install backdoors or persistent access points to maintain control over the system for future exploitation. To ensure ongoing communication and control, the attacker establishes command and control channels using methods like remote access, botnets, or hidden channels. The final stage involves the attacker carrying out their objectives, which could include stealing sensitive data and disrupting services., or compromising other systems within the network.

3. The diamond model

Sergio and others (Caltagirone, Pendergast, & Betz, 2013) recognized the limitations of linear cybersecurity intrusion models and aimed to address them by developing a more comprehensive approach. Their focus was to highlight specific hacker behaviors and establish a model that would enable cybersecurity professionals to identify the connections between attacker motivations, the victim, and the technology employed in an attack. This led to the creation of the diamond model in 2006, which was later published in 2013. In this model, each event, such as an intrusion, is depicted as a diamond shape divided into four quadrants, each representing essential aspects. These quadrants include the adversary, which refers to the persona of the individual or group launching the attack, the infrastructure comprising IP addresses, domain names, or email addresses, the capabilities of the adversary encompassing their tools and techniques like malware and exploits, and the victim encompassing individuals, services, network assets, or information. By utilizing the diamond model, cybersecurity professionals gain a more holistic understanding of cyber threats, allowing them to better analyze and respond to security incidents.

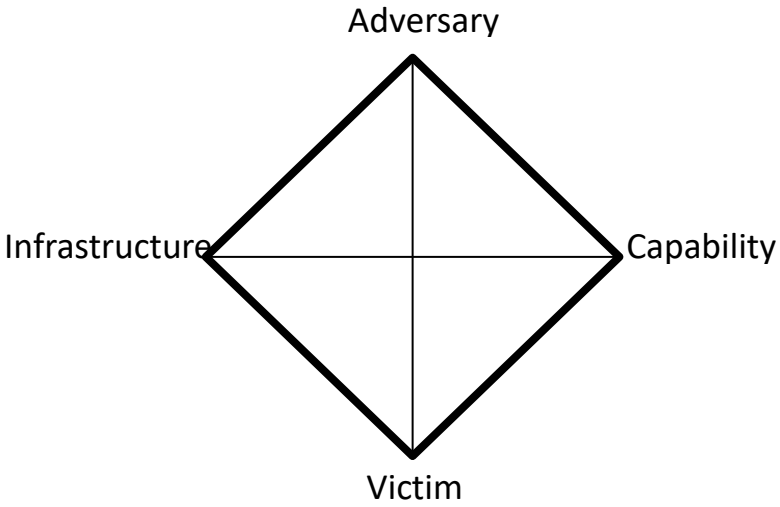

Figure 3: The Dimond Model

Source: (Caltagirone, Pendergast, & Betz, 2013)

Moreover, various theories have been proposed to explain the motivation behind cyberattacks. One such theory is the rational choice theory, which suggests that individuals are motivated to commit cyberattacks due to the potential rewards associated with successful attacks. Another theory is the social learning theory, which suggests that individuals learn and adopt cyber-attack behaviors through observation and interaction with others (Bachmann, 2008).

In summary, the theoretical literature on cyberattacks and their effect on the banking sector provides valuable insights into the various aspects of cyberattacks, theoretical frameworks for understanding the effects of cyberattacks, and theories that explain the motivation behind cyberattacks.

Cyber Attacks are malicious activities targeting computer systems and networks, such as the internet, to disrupt operations, steal data and information, and damage reputations (Li, 2017; Musman et al., 2008). These attacks can take various forms, such as denial-of-service attacks, phishing, malware infections, and ransomware attacks(Agrafiotis et al., 2018). Additionally, attackers may exploit vulnerabilities in systems and networks to gain access to confidential data, such as passwords and financial information(Acharya & Joshi, 2020; Cashell, Jackson, Jickling, & Webel, 2004).

5.1.3. Cyber security in Ethiopia

The government has recognized Ethiopia's reliance on digital infrastructure and the potential dangers of cyber-attacks, which has taken steps to protect the country's financial sector. In 2017, the government developed the Critical Mass Cyber Security Requirement Standard (CMCSRS), which stated the need for a delicate balance between the risk and benefits of information systems (Information Network Security Agency, 2011). The standard also emphasized the importance of ensuring the security of organizational information systems to protect against cyber-attacks and minimize their effect on the country (Information Network Security Agency, 2011).

To further secure cyberspace in Ethiopia, the government has formulated a legal framework to combat cybercrime, including the Telecom Fraud Offence Proclamation No. 761/2012 (Abraha & Hailu, 2015; Tsion Mathewos, 2015). Additionally, the government has established the Information Network Security Agency (INSA) to deal with cyber security challenges related to the development of the financial sector and critical infrastructure (Abraha & Hailu, 2015) (Information Network Security Agency, 2011) INSA has also formed the ETHIO-CERT Cyber Emergency Readiness and Response Team, which is responsible for responding to cyber security incidents Furthermore. The government has developed and implemented a national information and communication technology policy and strategy that includes cyber security initiatives (Information Network Security Agency, 2011).

The government has also established the Financial Intelligence Service (FIS) of Ethiopia, formerly known as the Financial Intelligence Center, which is responsible for detecting and preventing money laundering and the financing of terrorism ('Financial intelligence center establishment Regulation no.171/2009 - National Bank', n.d.) The FIS is empowered to conduct investigations, collect information, and provide intelligence to law enforcement agencies('Financial intelligence center establishment Regulation no.171/2009 - National Bank', n.d.)

Despite these measures, there is still a need for a delicate balance between risk and benefit as the reliance on information systems increases organizations' vulnerability to cyber-attacks, which are becoming more complicated, dynamic, and destructive. Therefore, continuous efforts and improvements in cybersecurity governance, law enforcement, and capacity-building programs are necessary to keep Ethiopia's financial sector safe from cyber-attacks.

5.1.4. Financial Sectors and ICT in Ethiopia

The Ethiopian financial sector has undergone significant changes in recent years, with the introduction of digital finance and financial technology (fintech) playing a significant role. This section aims to provide an overview of the current landscape of the Ethiopian financial sector, focusing on the emergence of digital finance and fintech, and analyzing their effect on the sector.

The literature on digital finance and fintech highlights their potential to increase financial inclusion, reduce transaction costs, and improve access to financial services for individuals and businesses. Studies have shown that mobile banking, online banking, and digital payments can improve financial inclusion in low-income and rural areas (Triki & Faye, 2013b). The literature also emphasizes the importance of fintech innovation in creating new business models, enhancing customer experience, and improving efficiency in the financial sector(Triki & Faye, 2013b).

Current Landscape of the Ethiopian Financial Sector:

A review of the Ethiopian financial sector reveals that close to 570 businesses offer a wide range of digital finance, e-commerce, transport, sector-tech, and ecosystem services. Most companies operating in the digital space are still small, and few 'digital disruptors' have emerged with widespread market acceptance, a large customer base, and meaningful revenue generation. However, the expansion of financial technology in Ethiopia, such as payment cards,

implementation of ATMs and point-of-sale (POS) systems, mobile banking, internet banking, and mobile money services, has paved the way for digital payment mechanisms in the financial sector.

Roles of Digital Finance and Fintech:

The effect of digital finance and fintech in Ethiopia can be seen in the increased adoption of digital payment mechanisms, such as mobile money and online banking, which have made transactions faster, more secure, and more convenient for customers. Fintech start-ups have introduced different value-added services and partnered with financial institutions, expanding access to financial services and enhancing customer experience. However, the ecosystem is also highly affected by cyber-attacks nationwide and globally, highlighting the need for strong cybersecurity measures.

The emergence of digital finance and fintech in Ethiopia has transformed the financial sector by expanding access to financial services and improving customer experience. However, there is a need for continued investment in digital infrastructure and fintech innovation to enhance financial inclusion further, reduce transaction costs, and improve efficiency in the sector. The potential benefits of digital finance and fintech for the Ethiopian economy cannot be ignored, and policymakers and financial institutions should work together to leverage these technologies for sustainable economic growth.

5.1.5. Banks and cyber-attack in Ethiopia

Ethiopia's Information Network Security Agency states that more than 2000 cyber-attack attempts on the nation were thwarted in the current 2022/23 Fiscal Year quarter. (Information Network Security Agency, 2011) Banks have become increasingly targeted by cyber-attacks in recent years. As such, the financial sector is highly exposed to cyber risk. (Temesgen, 2022).

The banking sector in Ethiopia has undergone a digital revolution in recent years, with the introduction of various technological advancements such as online banking, mobile banking, and digital payments. However, these technological innovations have also increased cybersecurity risks, particularly for financial institutions like banks. Cyber-attacks can pose a significant threat to the Confidentiality, Integrity, and Availability of information, which are the three main aspects

of information security. Therefore, it is crucial to understand the risks associated with cyber-attacks and their effects on financial institutions in Ethiopia.

According to recent studies, financial institutions are among the most targeted organizations by cybercriminals (Entrust, 2021; Rao, 2019). Banks, in particular, are more vulnerable to cyber-attacks due to their sensitive financial information making them prime targets for cybercriminals (Temesgen, 2022) Cyber-attacks on the banking sector can be categorized into two main types: targeted and untargeted attacks. Targeted attacks are designed to exploit a particular vulnerability in a system, while untargeted attacks are more general and opportunistic.

Cyber-attacks' effects on financial institutions are diverse and can have short-term and long-term consequences. Business disruptions resulting from cyber-attacks can lead to direct revenue losses for financial institutions. Fraudulent activities can result in direct financial losses, while data breaches can lead to reputational damage and litigation costs(Bouveret et al., 2018; 'Estimating Cyber Risk for the Financial Sector,' n.d.) Moreover, loss of customer trust due to a cyber-attack can have long-term effects on the financial institutions' operations and reputation.

5.2. Review of empirical literature

Empirical Literature Review:

The fact that the effect of cyber-attacks on financial sectors, such as banks, is an under-researched area compared to global studies indicates that there is a lack of understanding of the effect of cyber threats on the financial industry. Despite the increasing frequency and severity of cyber-attacks, there is limited research on how they affect financial institutions, their customers, and the broader economy.

One possible reason for this lack of research is that the financial industry may not be as transparent as other sectors, making it difficult for researchers to obtain data on cyber-attacks and their consequences. Additionally, financial institutions may not want to disclose the full extent of cyber-attacks for fear of damaging their reputation or losing customer trust. Another reason could be the complexity of the financial sector itself. There are many different types of financial institutions, and each may have unique vulnerabilities and responses to cyber-attacks. Therefore, researching the effect of cyber-attacks on the financial sector requires a nuanced approach considering the diverse financial institutions and their particular circumstances.

Irrespective of the scarcity of study, it is evident that cyberattacks seriously threaten financial stability. There are not many studies on the topic or at least closely related ones. The following are the empirical reviews of some of the related works.

Author	Finding
Abiye Weretaw (2012)	Abiye conducted a study on information security culture in the banking sector in Ethiopia. The research aimed to investigate the level of information security culture among bank employees and the factors that affect adopting information security practices. The findings revealed that a lack of awareness, inadequate training, and insufficient budget were vital factors hindering the adoption of information security practices in the banking sector. (Woretaw & Lessa, 2012)
Halefom Hailu (2015)	Halefom investigated the state of cybercrime governance in Ethiopia. The research aimed to identify the challenges facing the government and the private sector in preventing and mitigating cybercrime in Ethiopia. The study found that inadequate legal and institutional frameworks, lack of public awareness, and limited resources were crucial challenges facing the country in addressing cybercrime. (Abraha & Hailu, 2015)
Tesfaye Asfaw (2018)	Tesfaye developed a Cyber Security Auditing Framework (CSAF) for the banking sector in Ethiopia. The research aimed to provide a comprehensive framework for auditing the cyber security posture of banks in Ethiopia. The study found that the CSAF framework could help banks identify their cybersecurity weaknesses and develop effective strategies to mitigate cybersecurity risks. (Asfaw et al., 2018)
Tsion Mathewos (2015)	Tsion conducted a study on cybercrime in Internet banking activities in Ethiopia. The research aimed to investigate the types of cyber threats facing banks in Ethiopia and the measures banks took to mitigate these threats. The study found that phishing attacks, malware, and social engineering were some of the most common cyber threats facing banks in Ethiopia. The study also revealed that banks in Ethiopia had implemented various measures to mitigate these threats, including firewalls, antivirus software, and employee training. (Tsion Mathewos, 2015)

Author	Finding
Gardachew Worku (2010)	Gardachew conducted a study on electronic banking in Ethiopia. The research aimed to investigate the current state of electronic banking in Ethiopia and identify the sector's opportunities and challenges. The study found that the adoption of electronic banking in Ethiopia was still in its early stages and that a lack of infrastructure, limited internet connectivity, and low levels of financial literacy were some of the critical challenges facing the sector. (Worku, 2010)
Abel Temesgen (2022)	The paper "Cyber-Attack Vulnerability and Its Implication towards Digital Economic Development in Ethiopia" by Abel Temesgen investigates the vulnerability of Ethiopia to cyber-attacks and their impact on the digital economy. The study reveals poor password management, inadequate antivirus usage, and insufficient knowledge of cyber-attacks among digital economy users. Service providers exhibit shortcomings in product security and response to breaches. Recommendations include improving password practices, regular software updates, and awareness campaigns(Temesgen, 2022).

1. Table 2.1: Empirical Literature Review

Source: Literature Review

In conclusion, these six studies conducted in Ethiopia reveal various challenges facing the banking sector in addressing cyber security risks, including inadequate awareness and training, limited resources, and insufficient legal and institutional frameworks. However, the studies also highlight opportunities for improving cyber security, such as developing comprehensive cyber security auditing frameworks, using electronic banking, and adopting effective information security practices.

Main arguments: The six studies reveal various challenges and opportunities for improving cyber security in the banking sector in Ethiopia. These challenges include inadequate awareness and training, limited resources, insufficient legal and institutional frameworks, and low levels of cyber-financial literacy. The opportunities for improving cyber security include the development of comprehensive cyber security auditing frameworks, using electronic banking, and adopting effective information security practices. The findings suggest that cyber security in the banking sector in Ethiopia is still in its early stages and requires significant improvements.

Premises/assumptions: The six studies conducted in Ethiopia provide a comprehensive understanding of the challenges and opportunities for improving cyber security in the banking

sector. The findings of the studies are based on the specific context of Ethiopia and may / may not be generalizable to other contexts. Nevertheless, this perspective can also be seen as the issue of cyber security being more generic to all institutions, regardless of their size and type. According to the researchers of this paper, the financial sector is highly targeted to cyber-attacks because criminals primarily focus on financial gains and follow the money.

Context/background: Cybersecurity is a critical concern for the banking sector worldwide, and the banking sector in Ethiopia faces various challenges in addressing cybersecurity risks. The six studies were conducted to investigate the current state of cyber security in the banking sector in Ethiopia.

Significance/implication of the arguments: Their arguments suggest that significant improvements are required to address cyber security risks in the banking sector in Ethiopia. The findings of their studies can inform the development of policies and strategies to improve cyber security in the banking sector in Ethiopia. Regarding logical fallacy/inconsistency in their arguments is none apparent.

Approach/method/data used: The studies employed various methods, including surveys, interviews, and literature reviews, to investigate the challenges and opportunities for improving cyber security in the banking sector in Ethiopia. Even though the studies are based on the specific context of Ethiopia's financial sector and may not be generalizable to other contexts, the studies provide a comprehensive understanding of the challenges and opportunities for improving cyber security in the banking sector in Ethiopia. The approach taken in the studies is consistent with the assumption that the findings are based on Ethiopia's specific context and the financial sector. The approach taken in the studies has not been explicitly evaluated. The studies used various data sources, including surveys, interviews, literature reviews, criminal cases, and cyber law research.

Findings/observations/insights: The studies reveal various challenges and opportunities for improving cyber security in the banking sector in Ethiopia, including the need for adequate awareness and training, the development of comprehensive cyber security auditing frameworks, and the adoption of effective information security practices. The findings of the studies support the arguments that significant improvements are required to address cyber security risks in the banking sector in Ethiopia. Regarding the generalizability of the findings, the findings of the studies may or may not be generalizable depending on other contexts; on the one hand, according to research by the international monetary fund (Bouveret et al., 2018) there is a contagion effect

of cyber-attacks, and their span of influence targets everyone on the internet. On the other hand, some nations' cyber security posture and culture might be more resistant to cyber-attacks.

Research gaps: The above studies (Table 2.1) may have focused on specific aspects of cyber security in the banking sector, neglecting other major dimensions i.e., the technical aspect of the cyber security itself. The other gap is Some studies may have relied heavily on theoretical frameworks and literature reviews, lacking empirical data from real-world cases or practical insights. This limits the applicability and reliability of the findings. Therefore, these issues need to be addressed and that is the primary objective of this study.

5.3. Conceptual framework

To elaborate on the effect of cyberattacks on banks, the following figure is depicted by adopting the CIA framework to show the relationship between different variables of this research study. In the given framework, the independent variables are the compromise of Confidentiality, compromise of Integrity, and compromise of Availability. The dependent variable is the bank's business ICT system, and it shows the possible target of cyber-attacks that could target banks' financial systems. For the measurement scale and questionnaires, this research adopted the metrics used by Jasber Kaur and Norliana Mustafa (Kaur & Mustafa, 2013), and as of the categorization, it adopted the 20 cyber security controls standardized by NIST SP 800 – 53. And Halefom Hailu Abraha, in his study on the state of cybercrime governance in Ethiopia. The instrument was designed to evaluate how the cyber-attacks affect the security triad concerning the banks' ICT systems, namely Confidentiality, Integrity, and Availability.

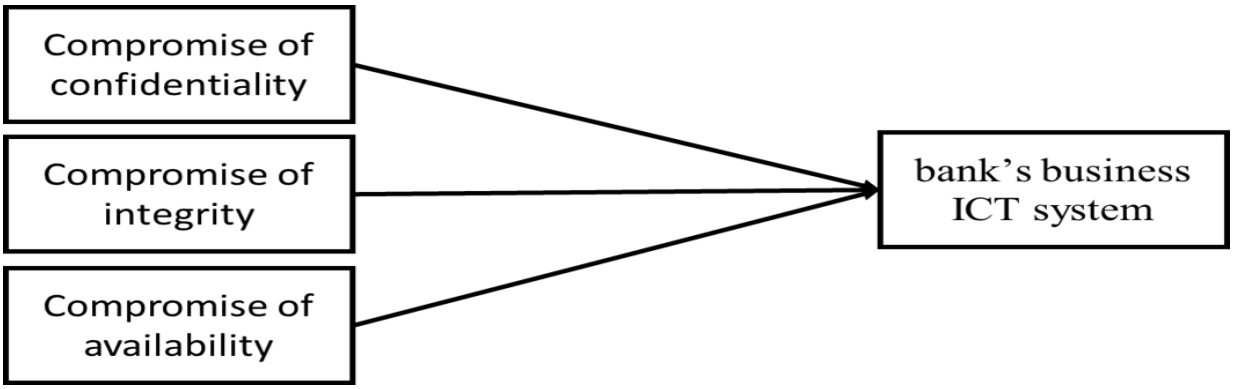

Figure 4: Conceptual Framework

Source: Adopted from NIST SP 800-53 and Kaur and Mustafa (2013)

Chapter Three

Research design and methodology

6.1. Description of the study area

The research on "The effects of cyber-attacks on banks Business ICT systems: The case banks in Ethiopia" aims to investigate the effect of cyber-attacks on banks in, Ethiopia. The study employed an explanatory mixed-methods research design that combines quantitative and qualitative data collection and analysis methods. The quantitative component of the study analyzed data collected from surveys administered to headquarters of banks' IT and cybersecurity experts, as well as data obtained from the Ethiopian CERT and cyber security auditing team from INSA (Information Network Administration). The qualitative component of the study employed a thematic analysis and an interpretive approach to gain a deeper understanding of the experiences and perspectives of top management, technical leaders, and experts who observe the effects of first-hand cyber-attacks in Ethiopia. Data for the qualitative component was collected through semi-structured interviews with selected INSA's cybersecurity experts and managerial staff. The study analyzed the collected data using statistical and content analysis techniques. Sample size and data availability are the significant limitations that the study faced, which may affect the depth and scope of the study.

6.2. Research approach

Creswell also discusses research approaches (Creswell & David Creswell, 2018) as the specific techniques and tools used to gather and analyze data. The chosen approach depended on the research questions, the data collection type, and available resources. Some common research approaches include:

The research approach suitable for this research thesis is a mixed-method approach, combining qualitative and quantitative methods. Surveys and interviews are the two methods that can be used in this research. The survey allowed the collection of quantitative data, and interviews allowed the collection of qualitative data. A mixed-method approach provided a more comprehensive understanding of the effect of cyber-attacks on banks in Ethiopia, allowing for both numerical and descriptive analysis.

This study uses a mixed research approach combining quantitative and qualitative data analysis methods. Quantitative analysis is appropriate for exploring the compromise of confidentiality, compromise of integrity, and compromise for availability dimensions of cyber security. On the other hand, qualitative methods provide detailed and valuable information about experts' perceptions, ideas, and experiences regarding specific topics or circumstances in their professional experience. The study aims to involve various stakeholders, including division leaders, team leaders, supervisors, fintech providers, and financial service providers in the sector.

6.3. Research design

The chosen research design, which is an explanatory mixed-methods approach, is well-suited to address the research objectives of the study. The quantitative component, conducted through surveys and data analysis, helps in providing descriptive information about the characteristics of cyber-attacks on banks' Business ICT systems in Ethiopia. This quantitative data allows for a systematic understanding of the types and frequencies of cyber-attacks.

The qualitative component, conducted through interviews and document analysis, delves deeper into the underlying reasons and experiences related to the impact of cyber-attacks. It helps in explaining the cause-and-effect relationship between compromises of confidentiality, integrity, and availability of business ICT systems in banks. The qualitative data provides valuable insights into the experiences, perspectives, and challenges faced by banks in dealing with cyber-attacks.

By combining both quantitative and qualitative methods, the research design enables a comprehensive understanding of the effects of cyber-attacks on banks' Business ICT systems in Ethiopia. The quantitative data offers a broad overview, while the qualitative data adds depth and richness to the findings. This mixed-methods approach allows for triangulation of data, enhances the validity of the research, and provides a more holistic understanding of the research topic.

6.4. Data source and type

The population of a study refers to the entire group of individuals, objects, or events that the researcher is interested in studying and making inferences about. The focus of the study is on the population consisting of the Information Network Security Administration (INSA) headquarters of banks in Ethiopia.

Professionals and including managers (division heads), team leaders, supervisors, cyber security experts, financial technology users, security testers, and employees working for the indicated firm, are the study's targeted population group. In addition to individuals, a four-year report document was also analyzed.

6.5. Sampling techniques and sample size

Sampling is selecting a representative subset of individuals, events, or an observation group from a larger population to participate in a research study (Neuman, 2014) to make inferences or draw conclusions about the population.

The survey was distributed to all headquarters' ICT and cybersecurity departments of major banks in Ethiopia, employing a census sampling technique. Census sampling is a method in which every member of the population is included in the sample, ensuring a comprehensive representation of the entire population (Neuman, 2014). In this study, the aim was to collect data from all relevant individuals within the target population, rather than selecting a subset. The questionnaire was distributed to 21 banks and 100 respondents participated in the survey.

As for the interview, three major departments were identified according to their direct relation to the issues and interviewed three individuals from the information network security administration.

Therefore, in this research, the census sampling technique was chosen to survey all the headquarters' ICT and cybersecurity departments of major banks in Ethiopia, ensuring a comprehensive representation of the population of interest. Among those, some banks did not respond.

6.6. Data collection instrument

Data collection and methodology are essential components of any research study. According to (Creswell & David Creswell, 2018), researchers must carefully select and apply appropriate methods for collecting and analyzing data to ensure the validity and reliability of their findings. This involves deciding the sampling strategy, data collection instruments, and data analysis techniques. The goal is to obtain accurate and meaningful data that can answer the research questions and contribute to the existing knowledge in the field. A similar measurement scale was

applied by(Kaur & Mustafa 3013). This section describes the data collection and methodology employed in the study on the effect of cyber-attacks on banks in Ethiopia.

6.6.1. Data source and collection techniques

Data sources and collection techniques refer to the methods and tools used to obtain information and data for research purposes (Creswell & David Creswell, 2018). The choice of data sources and collection techniques depends on the research question, the type of data required, and the resources available. When studying "The effect of cyber-attacks on banks in Ethiopia," questionnaires can be a dependable and effective way to collect data. Questionnaires are widely used in research as they can gather a considerable amount of data from a large sample of participants in a relatively short period. In this study, questionnaires were given to employees of INSA and banks.

6.6.2. Primary data sources

Primary data sources refer to information and data that are collected directly from the source for a specific research project. These sources can include questionnaires, interviews, and surveys. Primary data sources are often used when existing data sources are unavailable, or the researcher wants to obtain first-hand information about a particular phenomenon (Creswell & David Creswell, 2018). In this study, primary data was collected using questionnaires from INSA and banks and interviews with employees of INSA. Thematic coding is used for the qualitative data analysis technique to identify, categorize, and analyze patterns or themes within the dataset. It involves systematically organizing and labeling segments of data, such as interview transcripts, notes, or survey responses, based on their content or meaning. This allowed the researcher to obtain specific and detailed information on the effect of cyber-attacks on banks in Ethiopia from those with direct experience and knowledge of the subject.

6.6.3. Secondary data sources

Secondary data sources, on the other hand, refer to information and data collected by someone other than the researcher. These sources can include books, academic journals, reports, and databases. Secondary data sources are often used in research when the researcher wants to examine existing data to answer research questions or to provide context for primary data sources (Creswell & David Creswell, 2018). This study obtained secondary data from annual reports from INSA CERT and cyber security teams. A five-year report was thoroughly analyzed for this research.

These reports can provide a comprehensive overview of cyber-attacks on banks in Ethiopia and can provide additional context to the primary data collected through questionnaires and interviews.

6.7. Measurement

For the measurement scale and questionnaires, this research adopted the metrics used by Jasber Kaur (Kaur & Mustafa, 3013)and Norliana Mustafa, and as of the categorization, it adopted the 20 cyber security controls standardized by NIST SP 800 – 53. And Halefom Hailu (Abraha & Hailu, 2015) in his study on the state of cybercrime governance in Ethiopia. The instrument was designed to evaluate how cyber-attacks affect the security triad, namely confidentiality, integrity, and availability concerning the bank ICT systems. The instrument consists of 30 items. This instrument contained a five-point Likert scale to measure types of cyber-attack, compromise of confidentiality, compromise of integrity, and compromise of availability attributes in banks. The other set of questions is included to identify the major types of cyber-attack and identify the major ICT assets that are crucial for the continuity of business operations of the banks. The scale refers to 1 as strongly disagree to 5 as strongly agree.

6.8. Methods of data analysis

Data analysis and interpretation refer to analyzing and making sense of the data collected in a research study. This research applied both quantitative and qualitative approaches to data analysis. Quantitative data were collected from questionnaires and yearly reports and analyzed using descriptive and inferential statistics. The descriptive analysis of research involves examining the data's characteristics, such as central tendency and variability, while inferential analysis focuses on testing and making predictions about a larger population based on a sample(Creswell & David Creswell, 2018).

Qualitative data collected from in-depth interviews were analyzed using a thematic analysis approach. The thematic analysis involves identifying patterns, themes, and trends in the data to understand the underlying meanings and experiences of the participants (Braun amp, 2006). The qualitative analysis provided a more in-depth understanding of the effect of cyber-attacks on banks in Ethiopia from the employees' perspectives.

IBM SPSS version 27 software was used for quantitative data analysis since it is a powerful statistical tool that provides accurate and reliable results(IBM, 2023). Tables and charts present the quantitative findings, including frequencies, percentages, and correlations. The results of the qualitative analysis were presented in the form of narrative descriptions and quotes to support the findings.

6.9. Model specification

The equation of regressions in this study is generally built based on two sets of variables, namely the dependent variable (bank's business operation ICT system) and independent variables cyber security triads (Compromise of confidentiality, Compromise of integrity, and Compromise of availability). The primary objective of using regression equation in this study was to make the study more effective at describing, understanding, and predicting the stated variables.

$Yi = \beta 0 + \beta 1X1 + \beta 2X2 + \beta 3\ X3 + \varepsilon$

Where: Y is the outcome or dependent variable bank's business operation ICT system

X1= Compromise of Confidentiality,

X2 = Compromise of Integrity,

X3 = Compromise of Availability

β0, β1, β2, and β3 are the coefficients associated with each independent variable which measures the change in the mean value of Y per unit change in their respective independent variables ε represents the error term.

6.10. Validity and reliability

In this study, several measures were taken to ensure the validity and reliability of the data. The researcher used a purposive sampling technique to select participants who are knowledgeable about the effect of cyber-attacks on banks in Ethiopia, further enhancing the validity of the data. The researcher also used a coding system to analyze the qualitative data, ensuring that the themes and patterns identified were consistent across the data(Creswell & David Creswell, 2018).

The content validity index and Cronbach's alpha coefficient were used to test the validity and reliability of the scales as measures of the study conceptions. The questionnaire was distributed to practitioners and experts in the field for validation. Cronbach's alpha coefficient was used to test the internal consistency of variables in the research scale. The closer Cronbach's alpha is to 1, the higher the internal consistency reliability(Uma Sekaran, 2006). Using this test, the relationships among the items would be reliable for further analysis, and to ensure the quality of this research, a standardized questionnaire is used so that the instrument is already tested and valid.

Furthermore, conducting a preliminary study before the main research helped the researcher address any potential uncertainties related to the measuring instruments used for data collection. To achieve this, the researcher conducted a pilot survey involving 20 respondents who were not part of the study. Through this pilot survey, the researcher identified areas that required correction or adjustment in the data collection instruments. The researcher also consulted the advisor and other experts in the field on the issues.

By employing these measures, the study tried to produce valid and reliable data to draw a valid conclusion by providing a comprehensive understanding of the cyber-attacks effect on banks in Ethiopia.

Variable	No. of Items	Cronbach's Alpha
Compromise of Confidentiality	6	0.853
Compromise of Integrity	6	0.875
Compromise of Availability	6	0.842
Cyber-attack Type	6	0.80
Cyber-attack Severity	6	0.804
ICT Infrastructure	5	0.795

2 Table: 2.2 Reliability Test
Source: Survey result (2023)

6.11. Ethical consideration

The ethical considerations of this study are of paramount importance to the researcher. Informed consent had to be obtained from each participant before collecting data. The privacy and Confidentiality of the respondents were strictly maintained throughout the study. It is crucial to ensure that participants are not harmed physically or mentally during the study and that all necessary measures are taken to prevent such harm. The data collected had to be used solely for this study, and the participants' identities had to be kept confidential at all times. Any information obtained had been handled professionally and had not been disclosed to any third party without the explicit permission of the participants. The researcher obtained a support letter from St. Mary's University to facilitate contacting the Information Network Security administration. By adhering to these ethical considerations, the researcher had to ensure that the study was conducted responsibly and ethically and that the rights and well-being of the participants were protected.

Chapter Four

Data presentation, analysis, and interpretation

7.1. Introduction

The research aims to study the effect of cyber-attack on the ICT systems of banks in Ethiopia. The target of the study was ICT staff, so they were the focus of the data analysis and the interpretation section of this chapter. The descriptive and inferential analysis data was collected through a close-ended questionnaire and interview. Among the target population of 104 respondents, 100 responses were replied giving a 96% response rate. This was made possible by the researchers' ongoing follow-up and the respondents' significant concern. The following section states the study's descriptive and inferential analysis results for each questionnaire section.

7.2. Demographic characteristics of respondents

Variable	Label	Frequency	Percent
Gender	Male	80	80.0
	Female	20	20.0
	Total	100	100.0
Age	30-40	71	71
	41-50	26	26
	51-60	3	3
	Total	100	100
Level of Education	Degree	88	88.0
	Masters	12	12.0
	Total	100	100.0
Profession	Engineer	9	9.0
	Developer	45	45.0
	Cyber Security	37	37.0
	Manager	9	9.0
	Total	100	100.0
Industry	Private Banks	24	24.0
	Government Banks	46	46.0
	Microfinance	5	5.0
	Government security	25	25.0
	Total	100	100.0

Variable	Label	Frequency	Percent
Experience	0-5	64	64.0
	6-10	33	33.0
	Above 15	3	3.0
	Total	100	100.0

3 Table: 4.1 Demographic Information of The Respondents

Source: Survey result (2023)

As shown in Table 4.1, men comprised most of the respondents. In particular, out of 100 responders, 80% and 20 are male and female, respectively. This implies that male ICT workers outnumbered female ICT workers.

According to the respondents' age distribution, 71% of respondents were between the ages of 30 and 40, followed by 26 of respondents between the ages of 41 and 50. Values for the age ranges of 51 to 60 are 3%. This suggests that the bank's majority of ICT staff are youth. The educational background of respondents indicated that out of 100 participants, 88 (88%) have a first degree, and the remaining 12% have a master's degree. According to the distribution of responses to the question about education level, most respondents hold a bachelor's degree or higher. In light of this, it is reasonable to conclude that the ICT staff of banks comprises educated people. The respondent's position in their ICT staff office is also considered in the demographic section of the study. Therefore, 45% of the respondents were developers, followed by 37 (37%) cyber security officers of the institution and 9 (9%) managers and engineers of the ICT division of the institution. These results showed that most respondents are in the position of developer and cyber security officers, which helps institutions be capable of being protective and are in line with the required technological advancement because of the developers.

The demographic features of the respondents also include the respondents' industry or working area. Thus, 46% of the respondents are workers in government banks, 24% are from the private bank sector, and a minor percentage (25% and 5%) of the respondents are from government security institutions and microfinance, respectively. Moreover, these ICT staffs have different working experiences in their respective institution. Among the respondents, those with a working experience of 0 to 5 years are 64%, followed by respondents with work experience of 6 to 10 years, and the least but the most experienced ICT staffs are 3 %. Overall, it is possible to say that the banks' ICT staff are males with good academic preparation who work in the ICT department and have experience of up to five years and more.

The demographic information analysis revealed several key findings. Firstly, most respondents were male, indicating a gender imbalance within the ICT workforce of the banks. Secondly, the age distribution showed that a significant proportion of respondents fell within the 30-40 age range, suggesting a relatively young workforce. Furthermore, the educational background analysis indicated that most respondents held a bachelor's degree, highlighting a well-educated ICT staff. In terms of positions, developers and cyber security officers constituted the majority, reflecting the importance of these roles in ensuring technological advancement and protection. Government banks had the highest representation among the respondents when considering the industry or working area. Lastly, the respondents exhibited varying levels of work experience, with the majority having 0-5 years of experience. These findings provide insights into the composition of the ICT staff in the banks, highlighting the need for continued professional development and a focus on addressing the gender imbalance in the industry.

7.3. Descriptive, thematic, and document analysis

According to Scott 1999 explained that for Likert scale data from 1 (Strongly disagree) to 5 (Strongly agree) if the sample is approximately normally distributed, the interpretation should be intended for a mean up to 2.8 is “Disagree,” mean between 2.9 and 3.2 is “Neutral”, and mean above 3.21 is “Agree. Therefore, the decision of each variable statistics is done based on these criteria. In the process of analyzing the data, the standard deviation was used. Small standard deviations (relative to the value of the mean itself) indicate that data are close to the mean whereas a large standard deviation (relative to the mean) indicates that the data points are distant from the mean. Standard deviation is a measure of how well the mean represents the data. All of the variables were measured using a five-point Likert scale where 1 stands for strongly disagree and 5 stands for strongly agree. Therefore, the interpretation is made using the mean of each variable the mean falls between the two ranges, hence if the mean approaches 1 the interpretation would be the respondents disagree on the raised issue or variable and if it approaches 5 the reverse would be true.

The thematic coding analysis provides a structured overview of the interview data, highlighting key themes and subthemes related to the research topic. The findings can contribute to a deeper understanding of the cyber-attacks faced by Ethiopian banks and the measures implemented to

address these challenges. Additionally, potential areas for further research are identified, which can guide future investigations to explore limitations and opportunities for improvement in cybersecurity practices. In the analysis of the interview data, thematic coding was utilized as a qualitative data analysis technique. The aim was to identify, categorize, and analyze patterns and themes within the dataset, allowing for a deeper understanding of the research topic. The following steps were undertaken to conduct the thematic coding:

The Ethiopian CERT (Computer Emergency Response Team) has provided a comprehensive 4-year cyber incident report, offering valuable insights into the state of cyber threats in Ethiopia. The document outlines various types of cyber incidents experienced during the specified period, providing a detailed analysis of the number of attacks and the sectors affected. The researcher focuses on cyber-attacks targeting the financial sectors, especially banks. This analysis aims to outline the evolving cybersecurity landscape in Ethiopian financial sectors.

7.3.1. Common cyber-attacks targeting banks' business ICT system

1. Quantitative analysis

Items	N	Mean	Std. Deviation
Phishing attack	100	2.90	1.096
(DDOS) attack	100	2.97	1.150
Ransomware attack	100	2.87	1.143
Web-based attack	100	2.87	1.143
Malware attack	100	3.14	.995
Spamming	100	3.75	.925

4 Table:4.2 Types of Cyber Attack
Source: Survey result (2023)

The aforementioned table shows that, on average, 3.75 of the 100 people surveyed agreed that the type of cyber-attack committed against their institution is spamming attack, followed by a malware attack with an average value of 3.14, the web-based attack is identified as an occurred type of cybercrime by average 2.87 of the respondents, ransomware attack by 2.87, while DDOS attack is experienced an occurrence as 2.97 average respondents agreed on it as the committed type of

cyber-attack, and the last identified cybercrime is a phishing attack with an average of 2.9 respondents. All in all, among the identified cyber-crimes committed against banks in Ethiopia spamming, is in the first rank, and malware attack is second while web-based attack, ransomware, DDOS, and Phishing attacks are identified as committed crimes nearly on the same level of agreement.

Items	N	Mean	Std. Deviation
Phishing attack	100	3.34	1.148
(DDOS) attack	100	3.68	1.136
Ransomware attack	100	3.48	1.259
Web-based attack	100	3.59	1.207
Malware attack	100	3.55	.925
Spamming	100	3.20	1.223

5 Table: 4.3 Severity of cyber attack
Source: Survey result (2023)

Referring to the above table, besides identifying the type of cyber-attack committed on selected financial institutions it is very crucial to assess which one of them is the most severe and which has the least damage to the institutions' ICT system. Hence, based on the survey result DDOS attack has severe damage to the ICT system of the institution with an average mean value of 3.68 respondents' agreement, followed by web-based type attack with an average mean value of 3.59, malware attack with 3.55, ransomware attack 3.48, lastly phishing and spamming with a mean value of 3.34 and 3.2 respectively. In conclusion, it is possible to say that the most severe attack from the identified is DDOS, and the least severe is spamming according to respondents' reports on the issue of severity.

Items	N	Mean	Std. Deviation
Core banking systems are the most important ICT systems in the bank	100	4.53	.822
Mobile banking applications are the most important ICT systems in the bank	100	4.42	.855
Data centers, storage, and servers are the most important ICT systems in the bank	100	4.56	.891
Security appliances (Firewalls, IPS, IDS, antivirus, and antimalware) are the most important ICT systems in the bank	100	4.47	.904
Business Intelligence (BI) tools are the most important ICT systems in the bank	100	2.91	.900

6 Table: 4.4 ICT system of the bank
Source: Survey result (2023)

According to the above survey result; respondents' average level of agreement on business ICT systems varies from the core elements to some augmented ICT components in the department as well as at the corporation level. Hence, on average 4.53 respondents agreed that the core banking system in the institution is the basic component that enables the business firm to deliver its basic service, in the course of executing fundamental functions of the firm data centers, storage devices, and servers enable the company to store huge amount of data as 4.56 average respondents reported. Besides having enough storage equipment, it is mandatory to install and use security appliances and software such as firewalls IPS, IDS, antivirus, and antimalware for the safety of the stored data regarding this issue 4.47 average respondents agreed. In addition to basic components, these financial institutions should have business intelligence tools as 2.91 average respondents agreed on it. In conclusion, business firms must have basic or core ICT systems for basic function and data security.

2. Thematic Analysis

The methodology employed in this study was thematic analysis, which aimed to analyze the responses from key stakeholders, including the CERT team leader, the cyber security officer, and the penetration tester. Thematic analysis is a systematic approach that involves several steps. Firstly, the researcher familiarized themselves with the data collected from the participants, which

included their responses related to cyber-attacks on banks' business ICT systems. Next, initial codes were generated to capture the key ideas and concepts emerging from the data. These codes were then grouped into themes based on their similarities and patterns. The researcher reviewed and refined these themes to ensure their accuracy and relevance to the research objective. Finally, a coding scheme was applied to organize the data and extract meaningful insights.

The findings of the analysis shed light on the common types of cyber-attacks that target banks' business ICT systems. The participants consistently identified phishing attacks, malware infections, Distributed Denial of Service (DDoS) attacks, and insider threats as prevalent attack vectors in the banking sector. This convergence of perspectives among the stakeholders emphasizes the significance of these types of cyber-attacks and their potential impact on the security and integrity of banks' ICT systems. By identifying these common attack vectors, organizations in the banking sector can better understand the specific threats they face and develop targeted strategies to mitigate the risks associated with them.

3. Document Review

Cyber-attacks in the past three years (2011,2012,2013)

Type of attack	Total	Percent of total attack
1. Website attack	881	25.87%
2. Malware	657	19.29%
3. Infrastructure Scan	1142	33.53%
4. Infiltrate (bypass)	706	20.73%
5. DDOS	10	0.29%
6. Social Media hacking	8	0.23%
7. Online fraud	2	0.06%
Total	**3406**	**100.00%**

7 Table: 4.5Cyber-Attack Types From 2011 - 2013

Source: CERT Report (2011-13)

The analysis of Table 14.17 provides crucial insights into cyber-attacks in Ethiopia from 2011 to 2013, encompassing various attack types such as malware, website attacks, infrastructure scans, system infiltrations, DDOS attacks, and cyber fraud. Notably, there were significant fluctuations observed across these attack categories during the examined period.

Malware, DDOS (Distributed Denial of Service) attacks, and web attacks have witnessed alarming percentage increases over the years, underscoring the significant threats they pose to banks and their operations. The data reveal a substantial rise in malware incidents, with a staggering percentage increase of 356% from 2011 to 2013. This highlights the urgent need for banks to implement robust security measures to combat unauthorized access, financial theft, and disruptions that can result from malware attacks.

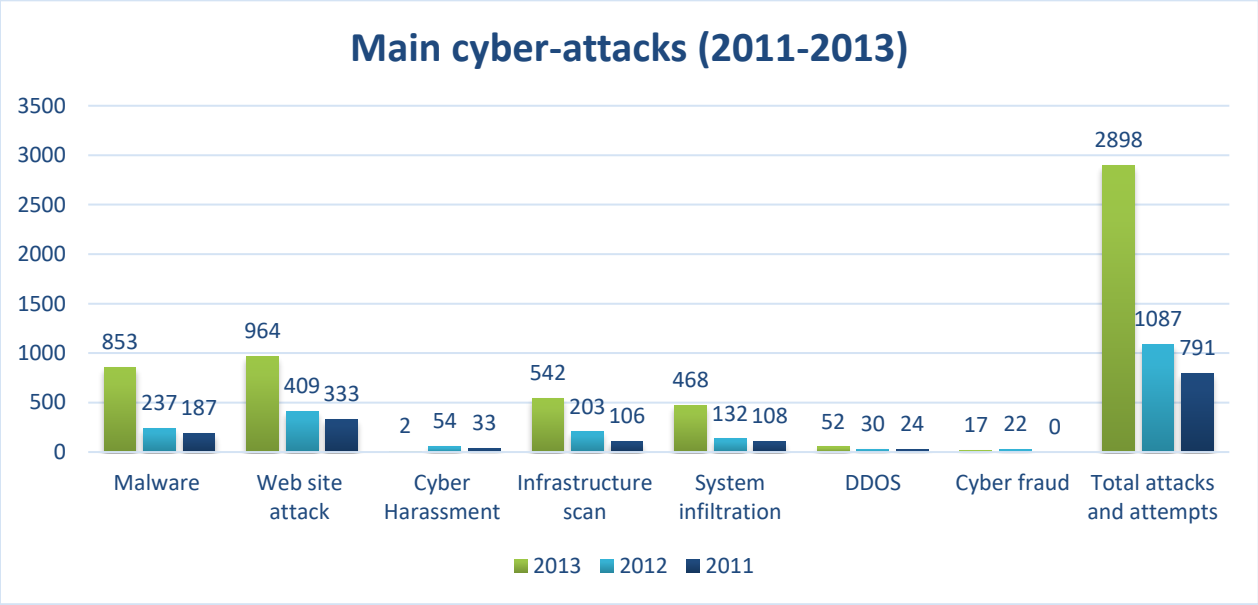

Figure 5: Cyber-Attack Types From 2011 - 2013

Source: CERT Report (2011-13)

Similarly, the data indicate a concerning trend in DDOS attacks, with a percentage increase of 116.7% over the same period. DDOS attacks can paralyze online services, rendering them

inaccessible to customers and causing financial losses. Such attacks not only disrupt banking operations but also tarnish the reputation and credibility of financial institutions. Therefore, banks must prioritize the implementation of advanced monitoring and mitigation techniques to safeguard against DDOS attacks and ensure uninterrupted access to their services.

Furthermore, web attacks demonstrate a substantial percentage increase of 189.6% during the three years. Web attacks exploit vulnerabilities in banking applications and can lead to data breaches, compromising sensitive customer information and eroding trust. Banks need to invest in robust web security measures, including regular vulnerability assessments, secure coding practices, and web application firewalls, to protect against these attacks and safeguard their customers' confidential information.

4. Implication:

The findings of the study reveal that cyber-attacks, such as phishing attacks, malware infections, DDoS attacks, and insider threats, have a significant impact on the financial performance of banks. This aligns with previous research, such as "The Effect of Cybercrime on a Bank's Finances" by Raghavan (2014) and "Impact of Information Security Breach on Financial Performance of Firms" by Myung Ko (2006), which highlight the adverse effects of cyber-attacks on the financial stability and profitability of financial institutions.

Phishing attacks, although not prominently detected in the survey findings, can have severe financial implications for banks if successful. Previous studies, such as "The Impact of Cyber Attacks on Private Firms' Cash Holdings" by Nurlana G (2021) and "The Effect of Cyber Attacks" by Arcuri (2018), emphasize the potential financial losses resulting from successful phishing attacks. This underscores the urgency of enhancing detection mechanisms and improving the reporting culture within banks to effectively mitigate the financial impact of phishing attacks.

Malware infections, DDoS attacks, and web attacks are identified as major cyber threats that can disrupt banking operations and compromise financial performance. These findings align with research conducted in "Cyber Attacks in the Banking Industry" by Adrash (2020) and "The Impact of Cyber Attacks on Financial Institutions" by Nida Tarik (2018), which highlight the detrimental effects of these attack types on the financial stability of banks. Therefore, financial institutions must allocate resources and prioritize cybersecurity measures to prevent and mitigate the financial repercussions of these attacks.

Implementing comprehensive security protocols, as recommended in "Cyber Security Measures in SMEs" by Milos (2015), can help banks protect their financial assets and minimize the financial impact of cyber-attacks. Advanced security measures such as firewalls, intrusion detection systems, and encryption technologies, as suggested in "Approaches to Modeling Impact of Cyber Attacks" by Alexander Kott (2018), are crucial in safeguarding financial systems and customer data. Regular security audits, as mentioned in "Cyber Security Auditing Framework (CSAF) for Banking Sector in Ethiopia" by Tesfaye Asfaw (2018), help identify vulnerabilities and enhance the overall security posture of banks.

Furthermore, building a strong cybersecurity culture within banks, as emphasized in "The Impact of Cybersecurity on SMEs" by Nabila A (2019), is essential for mitigating the financial impact of cyber-attacks. By providing comprehensive training programs and awareness campaigns, banks can educate employees about cyber threats and instill a sense of responsibility in adhering to security policies and procedures. This proactive approach, as highlighted in the literature, can significantly reduce the likelihood of successful cyber-attacks and minimize the resultant financial losses.

In conclusion, the findings of this study align with existing literature, indicating that cyber-attacks have a significant impact on the financial performance of banks. The implications drawn from the literature underscore the need for improved detection and reporting mechanisms for phishing attacks, as well as the implementation of comprehensive security protocols, regular security audits, and a strong cybersecurity culture within banks. By adopting these measures, banks can effectively mitigate the financial impact of cyber-attacks and safeguard their financial stability and profitability.

7.3.2. Compromise of confidentiality due to cyber attacks

The following analysis is conducted to examine the effect of the compromise of confidentiality on banks' business ICT systems due to cyber-attack

1. Quantitative analysis

Items	N	Mean	Std. Deviation
The compromise of confidentiality has a significant negative impact on the security of customer information, even in the event of a cyber-attack.	100	4.47	.745
The banks' measures to protect customer data from unauthorized access or disclosure are not fully effective against cyber-attacks.	100	3.87	1.022
The compromise of confidentiality due to cyber-attacks undermines the effectiveness of the banks' measures to ensure data security.	100	4.23	1.072
Cyber-attacks significantly impact the confidentiality of customer transactions within the banks' systems.	100	4.12	.967
The banks frequently encounter cyber-attack problems affecting the confidentiality of their business ICT systems.	100	3.99	1.176
Customer trust in the banks' ability to safeguard their confidential information is compromised by cyber-attacks.	100	3.72	.996

8 Table:4.6 Compromise of Confidentiality
Source: Survey result (2023)

The analysis of the above table provides valuable insights into the inverse relationship between the compromise of confidentiality and the banks' business ICT systems. According to the survey results, respondents indicated that the compromise of confidentiality has a significant negative impact on the security of customer information, even in the event of a cyber-attack (mean: 4.47). This implies that breaches in confidentiality can have severe consequences for the banks' critical business operations. Furthermore, the responses (mean: 3.87) suggest that the banks' measures to protect customer data from unauthorized access or disclosure are not fully effective against cyber-

attacks, indicating vulnerabilities in the security infrastructure. Additionally, respondents (mean: 4.23) expressed concerns that the compromise of confidentiality undermines the effectiveness of the banks' measures to ensure data security, highlighting the need for stronger safeguards. The survey results also indicate that cyber-attacks significantly impact the confidentiality of customer transactions within the banks' systems (mean: 4.12), posing risks to the confidentiality and privacy of sensitive data. Furthermore, the responses (mean: 3.99) suggest that banks frequently encounter cyber-attack problems affecting the confidentiality of their business ICT systems, indicating an ongoing and persistent threat. The analysis also reveals that customer trust in the banks' ability to safeguard their confidential information is compromised by cyber-attacks (mean: 3.72), which can lead to reputational damage and potential customer loss. These findings emphasize the critical importance of implementing robust security measures and continuously improving the banks' ICT systems to mitigate the risks associated with the compromise of confidentiality and ensure the protection of customer data.

2. Thematic Analysis

The analysis employed a thematic analysis methodology to examine the effect of cyber-attacks on the confidentiality of banks' business ICT systems. The responses of the interviewees, including the CERT team leader, the cyber security officer, and the penetration tester, were analyzed. The process involved familiarizing with the data, generating initial codes, grouping codes into themes, reviewing and refining themes, and applying a coding scheme. The findings revealed that cyber-attacks pose a significant threat to the confidentiality of banks' ICT systems. Unauthorized access and data breaches can compromise sensitive customer information and potentially lead to financial fraud. The interviewees discussed various measures to protect confidentiality, such as implementing robust encryption techniques, establishing access controls, and conducting user awareness programs. By conducting a thematic analysis and analyzing the responses of the interviewees, this study sheds light on the detrimental impact of cyber-attacks on the confidentiality of banks' business ICT systems. The identified threats underscore the importance of implementing effective security measures to safeguard sensitive information and mitigate potential risks. Measures such as encryption, access controls, and user awareness programs can contribute to strengthening the confidentiality of banks' ICT systems and ensuring the protection of customer data.

The thematic analysis highlighted the need for banks to prioritize cybersecurity and implement effective measures to mitigate the risks associated with cyber-attacks. It provided valuable insights into the challenges and vulnerabilities banks face in maintaining the confidentiality of their ICT systems. By understanding the potential consequences of cyber-attacks and implementing the recommended protective measures, banks can enhance their cybersecurity strategies and ensure the confidentiality of customer information.

Findings: The analysis revealed that cyber-attacks pose a significant threat to the confidentiality of banks' business ICT systems. The participants highlighted the risk of unauthorized access and data breaches, which could compromise sensitive customer information and lead to potential financial fraud. Measures to protect confidentiality, such as robust encryption, access controls, and user awareness programs, were discussed.

3. Document Review

Sectors affected by major cyber-attacks (confidentiality and integrity)

Targeted Institutions	Attacks from 2010 - 2014
1. Financial institute	84
2. Educational institutions	35
3. Security institutions	7
4. Government	89
5. Private Sectors	8
6. Media Institutions	85
7. Industry / Manufacturing	8
Total	316

Table 14.7: Sectors Affected by Cyber Attack

Source: CERT Report (2010-14)

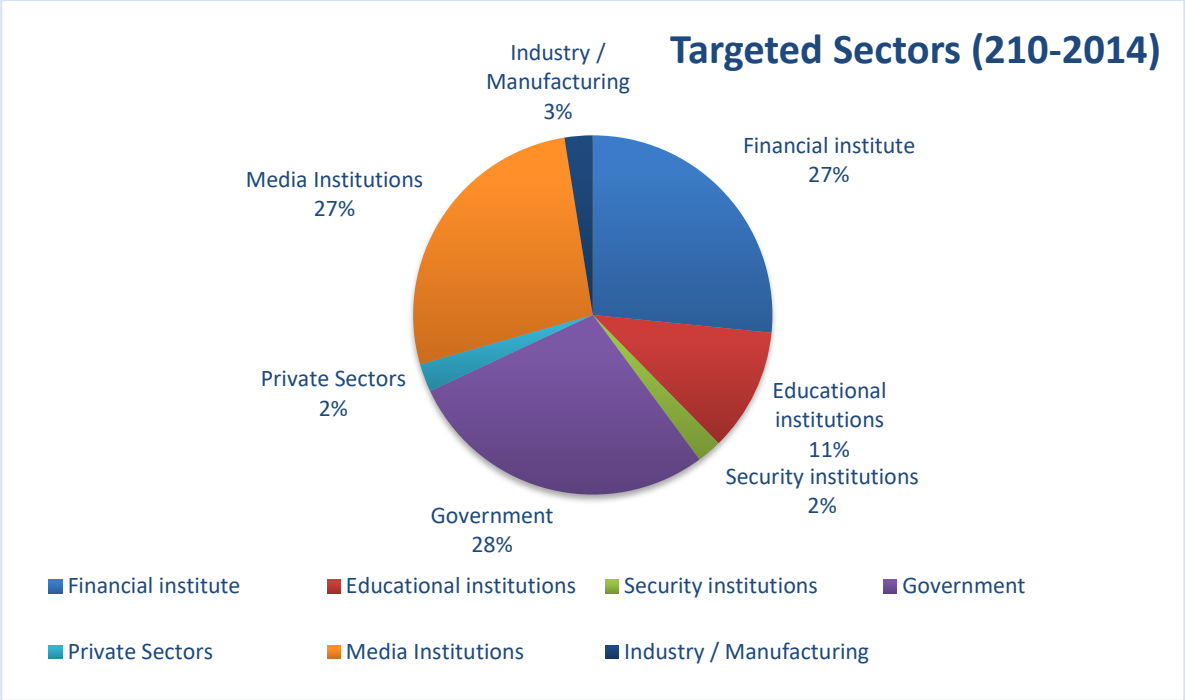

Figure 6:Sectors Affected by Cyber Attack

Source: CERT Report (2010-14)

The analysis of Table 2 indicates that the financial institution sector has been significantly impacted by cyber-attacks, representing approximately 26.6% of the total attacks reported between 2010 and 2014. Out of the 316 data(systems) confidentiality and integrity attacks documented during this period, financial institutions were targeted in 84 cases. These statistics highlight the alarming vulnerability of the sector to cyber threats. Cyber-attacks pose substantial risks to financial institutions, including financial losses, reputational damage, and compromised customer data.

4. Implication:

The compromise of confidentiality in banks' business ICT systems has significant implications for the banking industry. The negative impact on the security of customer information, even during cyber-attacks, highlights the need for robust security measures to protect sensitive data. These findings align with existing literature that emphasizes the importance of safeguarding customer information in the face of cyber threats (Analyzing Cyber Threats Affecting the Financial Industry, Anna, 2017; Cyber Attacks in the Banking Industry, Adrash, 2020; Threats to the Financial

Services Sector, PWC, 2014). Breaches in confidentiality can result in severe consequences, including financial fraud and reputational damage for financial institutions.

The persistent nature of cyber-attacks and their impact on the confidentiality of banks' business ICT systems is well-documented in the literature. Studies have shown that cyber-attacks pose risks to the integrity and privacy of sensitive data, with prior studies addressing these concerns (Cybercrime on Internet Banking Activities in Ethiopia, Tsion Mathewos, 2015). Additionally, the negative impact on customer trust due to cyber-attacks is supported by literature that emphasizes the importance of maintaining customer trust and confidence in the banking sector (The Impact of Cyber Attack on Brand Image, Kimberly A, 2017).

The thematic analysis further supports the need for proactive security measures to protect confidentiality. Recommendations for robust encryption, access controls, and user awareness programs align with the literature, which highlights these measures as essential for safeguarding customer data (Cyber Security Measures in SMEs, Milos, 2015). Furthermore, studies emphasize the importance of continuous monitoring and detection mechanisms in cybersecurity to maintain the integrity of banks' business ICT systems (Evaluating the Impact of Cyber Attacks on Missions, MITRE Corp, 2008).

The significant impact of cyber-attacks on the financial institution sector is demonstrated in the document review. This aligns with literature that identifies the financial sector as a prime target for cyber-attacks (Analyzing Cyber Threats Affecting the Financial Industry, Anna, 2017). Recommendations in the literature stress the need for financial institutions to allocate resources and invest in robust security measures to bolster their cybersecurity defenses (Approaches to Modeling Impact of Cyber Attacks, Alexander Kott, 2018).

Overall, the implications of the findings underscore the critical importance of implementing robust security measures, continuous monitoring, and collaboration among financial institutions, regulatory bodies, and cybersecurity experts. These measures align with existing literature that emphasizes the need for proactive cybersecurity strategies to protect customer data, maintain trust, and ensure the stability and trustworthiness of the financial sector. By aligning with relevant literature, this study strengthens the validity and reliability of the findings and provides practical insights for addressing cybersecurity challenges in the banking industry.

7.3.3. Compromise of integrity due to cyber attacks

The following analysis is conducted to examine the effect of the compromise of integrity on banks' business ICT systems due to cyber-attack

1. Quantitative analysis

Items	N	Mean	Std. Deviation
The accuracy and reliability of transactional data are compromised by cyber-attacks during transactions.	100	4.42	.819
Cyber-attacks significantly compromise the integrity of data stored in the bank's systems for online banking.	100	4.06	1.108
The bank's systems fail to effectively prevent unauthorized alteration or manipulation of data during cyber-attacks.	100	4.32	1.062
Cyber-attacks undermine the trustworthiness and reliability of the bank's data.	100	4.11	.920
The bank's data integrity for mobile applications is vulnerable to user-side cyber-attacks.	100	4.05	.925
Customer confidence in the accuracy and integrity of the bank's data is negatively impacted by cyber-attacks.	100	4.09	.944

9 Table: 4.8 Compromise of integrity
Source: Survey result (2023)

Like confidentiality, integrity is a crucial component of the business ICT system. The analysis examines the compromise of integrity within the bank's ICT system. According to the survey results, the majority of respondents agree that cyber-attacks significantly compromise the integrity of transactional data during transactions (mean = 4.42, SD = 0.819). Similarly, respondents indicate that the integrity of data stored in the bank's systems for online banking is compromised by cyber-attacks (mean = 4.06, SD = 1.108). The effectiveness of the bank's systems in preventing unauthorized alteration or manipulation of data during cyber-attacks is also perceived to be

compromised (mean = 4.32, SD = 1.062). Moreover, respondents agree that cyber-attacks undermine the trustworthiness and reliability of the bank's data (mean = 4.11, SD = 0.920). The integrity of the bank's data for mobile applications is seen as vulnerable to user-side cyber-attacks (mean = 4.05, SD = 0.925). Finally, respondents indicate that customer confidence in the accuracy and integrity of the bank's data is negatively impacted by cyber-attacks (mean = 4.09, SD = 0.944).

These findings suggest that the compromise of integrity has a significant impact on the bank's ICT system. Cyber-attacks are seen as posing a risk to the accuracy, reliability, and trustworthiness of transactional data, as well as data stored in the bank's systems. This compromise of integrity can lead to potential consequences such as data manipulation, unauthorized alterations, and loss of customer confidence. To address these issues, the bank must enhance its cybersecurity measures, strengthen data integrity controls, and implement proactive strategies to mitigate the risks associated with cyber-attacks and ensure the integrity of its ICT system.

2. Thematic Analysis

Methodology: Thematic Analysis was conducted to analyze the responses from the CERT team leader, the cyber security officer, and the penetration tester regarding the effect of cyber-attacks on the integrity of banks' business ICT systems. The analysis followed a systematic approach, starting with familiarizing with the data gathered from the participants. Initial codes were generated to capture the key ideas and concepts emerging from the responses. These codes were then grouped into themes based on their similarities and patterns. The themes were reviewed and refined to ensure their accuracy and relevance to the research objective. Finally, a coding scheme was applied to organize the data and extract meaningful insights.

Findings: The thematic analysis revealed that cyber-attacks pose a significant threat to the integrity of banks' business ICT systems. The participants identified potential risks related to the manipulation or alteration of transactional data, account balances, and critical financial information. Unauthorized modifications to these data were found to undermine the reliability and trustworthiness of the systems, leading to financial losses and regulatory non-compliance. The analysis highlighted the need for robust measures to ensure data integrity, such as implementing secure authentication protocols, employing encryption techniques, and regularly monitoring and auditing system activities. Additionally, participants emphasized the importance of maintaining an

up-to-date understanding of emerging cyber threats and continuously improving security measures to mitigate the risks to the integrity of banks' ICT systems.

By considering the objective "To examine cyber-attacks effect on the integrity of banks' business ICT systems," the thematic analysis provided valuable insights into the potential consequences of cyber-attacks on the integrity of these systems. The findings underscore the critical importance of implementing strong security measures to protect the accuracy and reliability of transactional data and financial information. Furthermore, the analysis highlights the need for ongoing vigilance and proactive measures to detect and prevent unauthorized modifications or alterations to critical data. By prioritizing data integrity and investing in robust cybersecurity practices, banks can mitigate the risks associated with cyber-attacks and maintain the trust and confidence of their customers.

3. Document Review

The examination of the impact of cyber-attacks on banks' business ICT systems was conducted through a document review using the CERT report. The findings revealed that cyber-attacks had a significant effect on financial institutions, accounting for approximately 26.6% of the total reported attacks from 2010 to 2014. Out of the 316 documented attacks on data confidentiality and integrity during this period, 84 specifically targeted financial institutions. The analysis of Table 2 further confirms the substantial impact of cyber-attacks on the financial institution sector, which accounted for around 26.6% of all reported attacks between 2010 and 2014. Out of the 316 attacks documented during this timeframe, financial institutions were the victims in 84 instances. These statistics highlight the sector's alarming vulnerability to cyber threats, with potential consequences including financial losses, reputational damage, and compromised customer data.

To mitigate these risks, financial institutions must allocate sufficient resources to strengthen their cybersecurity defenses. This involves investing in robust security measures, conducting regular risk assessments, and implementing comprehensive employee training programs. Additionally, fostering collaboration among financial institutions, regulatory bodies, and cybersecurity experts is crucial. This collaboration enables the sharing of information, the development of industry-wide best practices, and collective efforts to address emerging cyber threats. Protecting the financial

sector from cyber-attacks is vital not only for individual institutions but also for ensuring the stability and trustworthiness of the entire industry.

4. Implication:

The convergence of findings from the quantitative analysis, thematic analysis, and document review underscores the implications of cyber-attacks on the integrity of banks' business ICT systems. The survey results reveal a significant negative impact on the security and reliability of customer information, even in the face of cyber-attacks. These findings align with literature that emphasizes the vulnerability of financial institutions to cyber threats and the need for effective measures to protect data integrity (Quarib, 2021). The compromised integrity undermines the banks' efforts to safeguard data accuracy and reliability, highlighting the importance of robust security measures (Gardachew Worku, 2010).

The thematic analysis further supports these implications by emphasizing the risks posed by unauthorized manipulation or alteration of data. The discussion highlights the importance of secure authentication protocols, encryption techniques, and monitoring and auditing activities to protect data integrity (Milos, 2015). The literature also emphasizes the significance of these measures in maintaining the trustworthiness of customer information and preventing potential financial losses (Adrash, 2020).

The document review provides additional evidence of the vulnerability of financial institutions to cyber-attacks. This highlights the urgent need for financial institutions to invest in robust security measures and regularly assess risks (Nida Tarik, 2018).

In conclusion, the triangulation of data from different sources confirms the implications of cyber-attacks on the integrity of banks' business ICT systems. The findings align with existing literature, emphasizing the importance of robust security measures, continuous improvement of ICT systems, and employee training programs to protect the accuracy and reliability of customer data (ENTRUST, 2021). By incorporating relevant literature, this study strengthens the validity and reliability of the findings, providing practical insights for addressing cybersecurity challenges in the banking industry.

7.3.4. Compromise of availability due to cyber attacks

The following analysis is conducted to examine the effect of the compromise of confidentiality on banks' business ICT systems due to cyber-attack.

1. Quantitative analysis

Items	N	Mean	Std. Deviation
Mobile banking services are frequently disrupted and become non-functional during cyber-attacks.	100	4.54	.822
The bank's online services experience significant disruptions and unavailability during a DDoS attack.	100	4.30	.847
Cyber-attacks frequently cause disruptions and unavailability of critical banking services.	100	4.27	.802
The bank struggles to maintain uninterrupted access to its services in the face of cyber-attacks.	100	4.31	.800
The availability of online banking services is severely compromised by cyber-attacks.	100	3.85	.957
Customer convenience and access to banking services are significantly impacted by cyber-attacks.	100	3.63	1.070

10 Table: 4.9 Compromise of availability
Source: Survey result (2023)

The findings reveal that the majority of respondents expressed concerns regarding the compromise of availability during cyber-attacks. Specifically, the mean scores indicate that respondents generally agreed that mobile banking services are frequently disrupted and become non-functional during cyber-attacks (Mean = 4.54, SD = 0.822). Similarly, the bank's online services were perceived to experience significant disruptions and unavailability during a DDoS attack (Mean = 4.30, SD = 0.847). Respondents also agreed that cyber-attacks frequently cause disruptions and the unavailability of critical banking services (Mean = 4.27, SD = 0.802).

Furthermore, the results indicate that the bank struggles to maintain uninterrupted access to its services in the face of cyber-attacks (Mean = 4.31, SD = 0.800). The availability of online banking

services was perceived to be severely compromised by cyber-attacks (Mean = 3.85, SD = 0.957), and customer convenience and access to banking services were significantly impacted by cyber-attacks (Mean = 3.63, SD = 1.070).

Overall, the data suggest that respondents perceive a negative association between the compromise of availability and the bank's business ICT system. The findings highlight the potential challenges and disruptions faced by banking services during cyber-attacks, emphasizing the need for robust measures to ensure the continuous availability and functionality of these services.

2. Thematic Analysis

The researcher employed thematic analysis as the methodology to analyze the responses obtained from the CERT team leader, the cyber security officer and the penetration tester. This analytical approach involved various steps, including familiarizing with the data, generating initial codes, grouping codes into themes, reviewing and refining themes, and finally applying the coding scheme.

Through the analysis, the researcher discovered that cyber-attacks have a substantial impact on the availability of banks' business ICT systems. The participants highlighted the disruptive nature of these attacks, leading to prolonged system downtime, service disruptions, and loss of functionality. Specifically, Distributed Denial of Service (DDoS) attacks were identified as a major threat to system availability. To counteract these challenges, the participants emphasized the importance of having robust incident response plans in place, redundant infrastructure to ensure system resilience, and proactive monitoring to detect and mitigate the impact of cyber-attacks.

By examining the effect of cyber-attacks on the availability of banks' business ICT systems, the findings underscore the critical need for financial institutions to prioritize and invest in measures that enhance system availability. This includes developing comprehensive incident response strategies, implementing redundancy measures to minimize downtime, and continuously monitoring for potential threats. The research highlights the importance of adopting proactive security measures to ensure the uninterrupted functioning of banks' ICT systems and maintain the availability of essential services to customers.

3. Document Review

Trend analysis for the total number of attacks

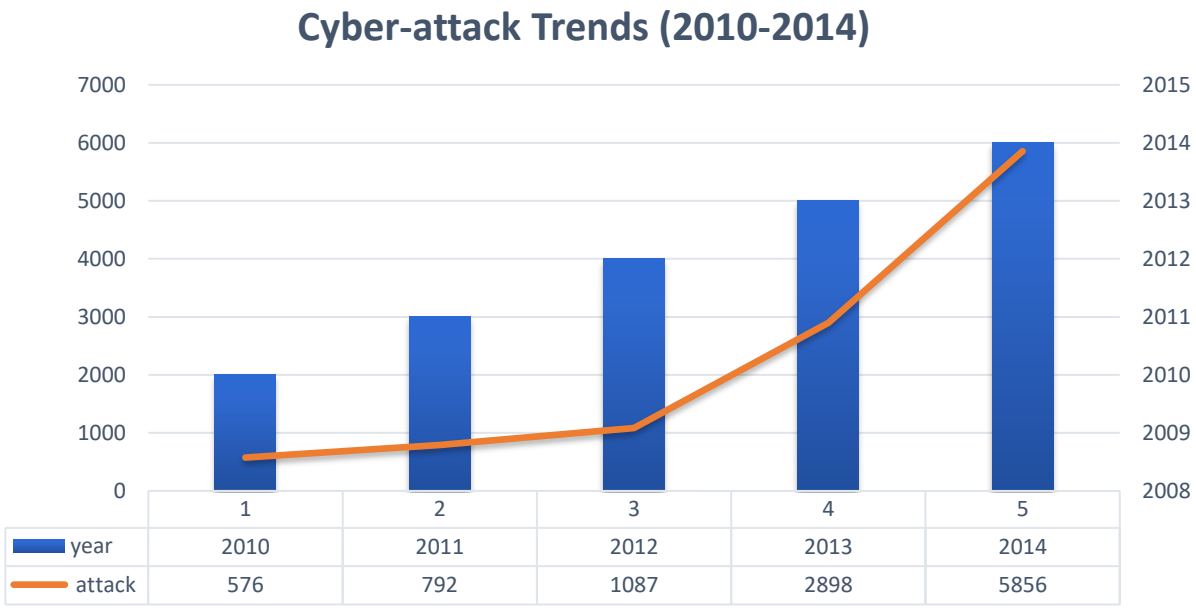

Figure 7: Cyber-Attack Trend Growth

Source: CERT Report (2010-14)

The data provided illustrates a significant increase in the number of cyber-attacks in Ethiopia from 2010 to 2014. The analysis of the cyber-attack trends from 2010 to 2014, as reported by CERT, reveals a significant increase in the total number of attacks over the years. In 2010, there were 576 reported cyber-attacks, which experienced a substantial jump to 792 in 2011. The upward trend continued in 2012, with 1087 attacks documented. The year 2013 witnessed a sharp surge in cyber-attacks, reaching a staggering total of 2898 cases. This upward trajectory persisted in 2014 when the number of reported attacks skyrocketed to 5856. A sudden increase in the volume or intensity of malicious traffic targeting a specific network or website. These escalating numbers underscore the escalating threat landscape in the realm of cybersecurity. Cyber-attacks have become more frequent and sophisticated, posing substantial risks to various sectors and industries. The growing frequency of cyber-attacks like DDOS emphasizes the urgent need for strong cybersecurity measures to protect banking ICT system availability. Vigilance, up-to-date security practices, and prioritizing cybersecurity are vital for safeguarding against potential threats. Proactive strategies should focus on maintaining uninterrupted system availability and defending against attacks that target system availability.

4. Implication:

The implications of findings regarding the compromise of availability in banks' business ICT systems have significant implications for the banking industry. The negative impact on the availability of critical banking services, such as mobile banking and online services, during cyber-attacks, highlights the need for robust measures to ensure uninterrupted access to these services. These findings align with existing literature that emphasizes the disruptive nature of cyber-attacks and their impact on system availability (Analyzing Cyber Threats Affecting the Financial Industry, 2017). Studies have shown that cyber-attacks frequently cause disruptions and unavailability of banking services, reinforcing the importance of addressing this issue (Cyber Attacks in the Banking Industry, 2020).

The thematic analysis further supports the impact of cyber-attacks on the availability of banks' business ICT systems. Key stakeholders in the field, including the CERT team leader, cyber security officer, and penetration tester, highlighted the disruptive nature of cyber-attacks and their consequences on prolonged system downtime and loss of functionality. Specifically, Distributed Denial of Service (DDoS) attacks were identified as a major threat to system availability. These insights align with literature that emphasizes the need for robust incident response plans, redundant infrastructure, and proactive monitoring to mitigate the impact of such attacks (Approaches to Modeling Impact of Cyber Attacks, 2018).

The document review provided a trend analysis showcasing the increasing number of cyber-attacks in Ethiopia over the years. The escalating numbers highlight the growing threat landscape in cybersecurity and the need for proactive strategies to combat these attacks. This finding resonates with literature that recognizes the evolving and sophisticated nature of cyber-attacks, emphasizing the urgent need for robust cybersecurity measures (Cyber Risk Landscape 2017, 2017).

The convergence of findings from the quantitative analysis, thematic analysis, and document review provides a comprehensive understanding of the effect of cyber-attacks on the availability of banks' business ICT systems. The perception of respondents regarding compromised availability during cyber-attacks, insights from key stakeholders, and the increasing trend of cyber-attacks over the years all contribute to establishing the significant impact of cyber-attacks on system availability. This alignment with relevant literature strengthens the validity and reliability of the research findings (The Impact of Cyber Attacks on Financial Institutions, 2018). It underscores the

importance of implementing measures to ensure the continuous availability and functionality of banking services, safeguarding the interests of customers and the stability of the banking sector (Banking on Cybersecurity White Paper, 2021).

7.4. Association and effect analysis

7.4.1. Relationship analysis between variables

To determine the existence and level of association, the study used bivariate correlation from which Pearson's correlation coefficient is considered. Pearson's correlation coefficient falls between -1.0 and +1.0, indicating the strength and direction of association between the two variables (Field, 2005). Pearson's correlation coefficient (r) was used to conduct the correlation analysis to find the level and direction of the relationships between the dependent and independent variables. It was also used to rank the variables that have the strongest associations with the bank's business ICT system. Correlations of 0.30 are regarded to mention worthy (Cohen, 1988). High correlation coefficients illustrate a higher level of association between the variables (i.e., dependent and independent). According to Cohen (1988), the value of Pearson's correlation is divided into three areas. A correlation coefficient between 0.10 and 0.29 indicated a weak correlation, a correlation coefficient between 0.30 and 0.49 indicated a medium correlation and a correlation coefficient between 0.50 and 1.0 indicated a strong correlation among the variables.

The bivariate correlation of a two-tailed test confirms the presence of statistically significant difference at probability level $p<0.05$ i.e., assuming a 95% confidence interval on statistical analysis. The Pearson correlation analysis shown in Table 4.8 below all independent variables (compromise of confidentiality, compromise of integrity, and compromise of availability) were significantly (statistically) and negatively correlated with the bank's business ICT system.

The correlation analysis table shows the correlations between the ICT system of the bank and three variables: compromise of integrity (COI), compromise of confidentiality (COC), and compromise of availability (COA). The correlation coefficient measures the strength and direction of the linear relationship between two variables. In this analysis, negative correlation coefficients indicate an inverse relationship, where an increase in one variable is associated with a decrease in the other variable, while positive correlation coefficients indicate a direct relationship, where an increase in one variable is associated with an increase in the other variable.

The correlation between the ICT system of the bank and the compromise of integrity (COI) is -0.661**. This negative correlation suggests that as the compromise of integrity decreases, the performance of the ICT system of the bank tends to decrease.

Similarly, the correlation between the ICT system of the bank and the compromise of confidentiality (COC) is -0.696**. This negative correlation indicates that as the compromise of confidentiality decreases, the performance of the ICT system of the bank tends to decrease.

The correlation between the ICT system of the bank and the compromise of availability (COA) is -0.432**. Again, this negative correlation suggests that as the compromise of availability decreases, the performance of the ICT system of the bank tends to decrease.

All of the correlations mentioned above are statistically significant at the 0.01 level, indicating a strong relationship between the variables. Overall, the correlation analysis suggests that there is a significant negative association between the performance of the ICT system of the bank and the compromise of integrity, confidentiality, and availability. This implies that as the compromise of these security aspects decreases, the ICT system's effectiveness and reliability tend to be adversely affected.

Correlations

		ICT system of the Bank	COI	COC	COA
ICT system of the Bank	Pearson Correlation	1			
	Sig. (2-tailed)				
	N	100			
COI	Pearson Correlation	-.661**	1		
	Sig. (2-tailed)	0.000			
	N	100	100		
COC	Pearson Correlation	-.696**	.726**	1	
	Sig. (2-tailed)	0.000	0.000		
	N	100	100	100	
COA	Pearson Correlation	-.432**	.609**	.620**	1
	Sig. (2-tailed)	0.000	0.000	0.000	
	N	100	100	100	100
**. Correlation is significant at the 0.01 level (2-tailed).					

11 Table: 4.10 Correlations between Dependent and independent variables
Source: Survey result (2023)

7.5. Assumption test in multiple linear regression

7.5.1. Normality test

The normal distribution is a fundamental statistical concept with significant implications for data analysis. A normal distribution with a mean of 0 and a standard deviation of 1 is referred to as a standard normal distribution (Garson, 2012). In this study, the researcher employed multiple regression analysis, which assumes that the variables in the sample follow a normal distribution. To ensure the validity of the findings, the normality assumption was assessed by examining the distribution of residuals, representing the differences between the observed values and the predicted values from the regression model.

The assessment of residuals revealed a bell-shaped form, with the data points distributed around a mean of zero, indicating adherence to the normal distribution assumption. This observation was further supported by the histogram displayed in Figure 5, which clearly depicted the characteristic shape of a normal distribution. Additionally, normal likelihood plots, specifically the normal p-plot, were utilized to confirm the assumption of normality. The normal p-plot, as shown in Figure 5, displayed a straight line, suggesting a close alignment between the observed data points and the expected values under a normal distribution.

The confirmation of normality through both the histogram and the normal p-plot strengthens the researcher's confidence in the normal distribution assumption and enhances the accuracy of the statistical inferences made regarding demographic parameters derived from the survey statistics. This careful consideration and validation of normality provide a solid foundation for the robustness and reliability of the data analysis in this study.

The sample's variables must have a naturally distributed distribution to use multiple regression analysis. Assume the residuals were normally distributed around the zero mean of the histogram and that it had a bell-shaped form. Figure 5 illustrates how the residuals were normally distributed and adhered to the normal distribution assumption, demonstrating that the findings were normally distributed.

Because the findings supported the data's assumed normalcy, it is likely that the inferences made about demographic parameters from survey statistics are accurate. Additionally, the normal likelihood plots were utilized to confirm the assertion of normality, as seen in Figure 8 of the normal p-plot.

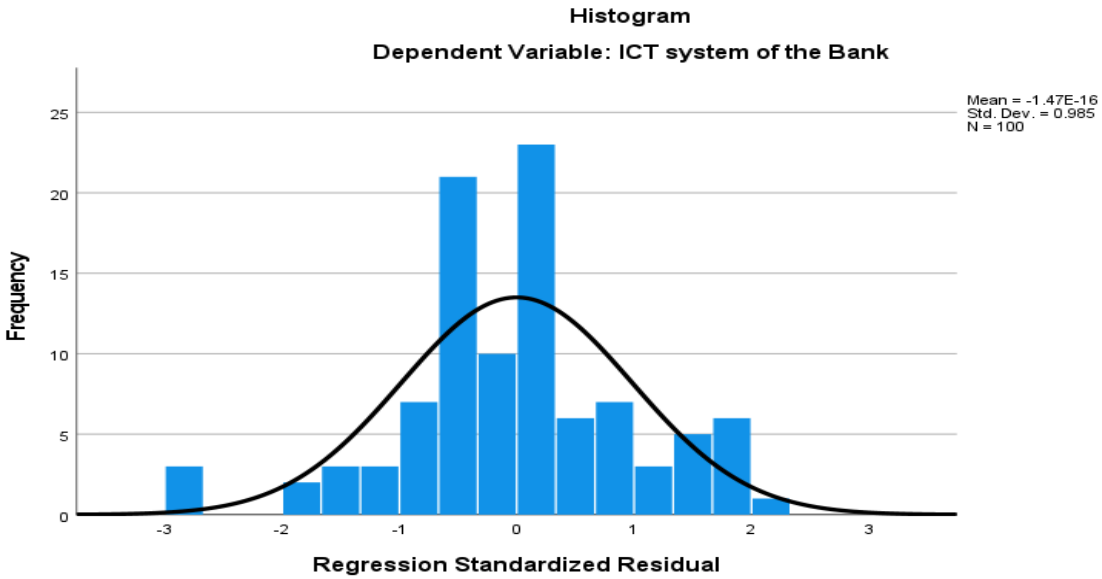

Figure 8: Normality Test, Histogram

Source: Survey result (2023)

7.5.2. Test of linearity

The normal probability plot (Chambers et al., 1983) is a useful visual tool for assessing the normal distribution of a dataset. By comparing the data points to a fitted distribution line, we can determine how well the observed data aligns with a theoretical normal distribution. In an ideal scenario, the points on the plot would fall nearly along a straight line, indicating a good fit. Any deviations from this straight line suggest a departure from normality.

Upon examining the normal probability plot, it is evident that the data exhibits a significantly linear structure. The discrepancies between the line fit and the probability plot points are minimal. Based on this plot, it appears that a normal distribution is a reasonable model for the data. The

linear trend observed in the probability plot further supports this conclusion. Moreover, the normal probability plot of the residuals confirms that the error terms are indeed normally distributed.

Overall, the analysis of the normal probability plot provides strong evidence for the normality of the dataset. The plot's linear structure and the consistency between the fitted line and the data points indicate a good fit for a hypothetical normal distribution. Similarly, the normality of the residuals supports the assumption of normal distribution for the error terms.

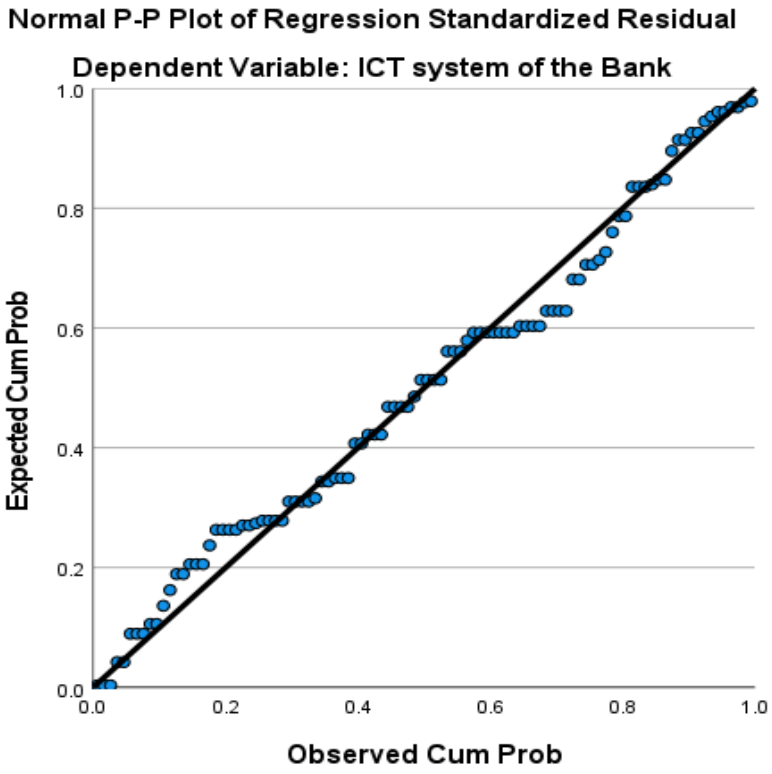

Figure 9: Normal P P-Plot

Source: Survey result (2023)

7.5.3. Test of homoscedasticity

The issue of heteroscedasticity, which assumes that the variance of the error terms should be constant, is a critical assumption in ordinary least squares. In this study, a scatter plot was used to test for heteroscedasticity. The standardized residuals (errors) were plotted on the Y axis, while the standardized predicted values of the dependent variable based on the model (ZPRED) were plotted on the X axis.

Upon examining the scatter plot, it is evident that there is no discernible pattern in the distribution of the residuals. This indicates the absence of heteroscedasticity in the data. The scatter plot does not exhibit any systematic relationship between the standardized residuals and the standardized predicted values.

Based on this analysis, it can be concluded that there is no evidence of heteroscedasticity in the dataset. The constant variance assumption of the ordinary least squares model holds, suggesting that the model is appropriate for the data.

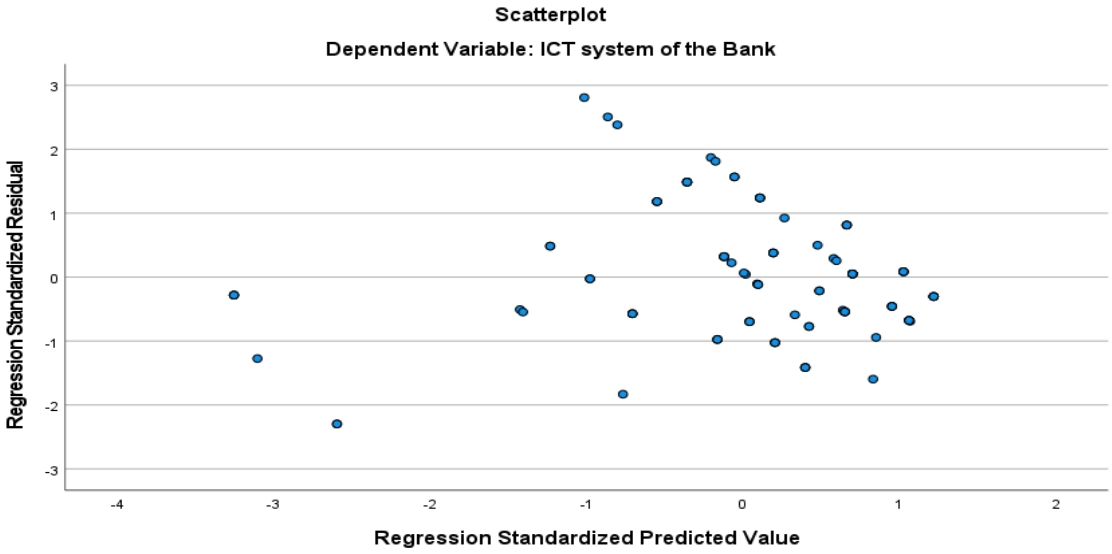

Figure 10: Test of Heteroscedastic

Source: Survey result (2023)

7.5.4. Test of multicollinearity

Multicollinearity refers to the presence of a nonlinear relationship between the dependent variable and each independent variable. To assess the assumption of multicollinearity in the regression model, the variance inflation factor (VIF) test was conducted in this study. The VIF test helps identify potential multicollinearity issues among the explanatory variables.

The results of the VIF test indicate that the maximum VIF value is 2.819. This value suggests that there is no significant multicollinearity issue among the explanatory variables. Generally, multicollinearity becomes a concern when the VIF value exceeds 10. Since none of the variables

in this study have a VIF value exceeding 10, it can be concluded that multicollinearity is not present in the data.

Based on these findings, it can be inferred that there is no evidence of multicollinearity among the variables included in the regression model. This suggests that the variables are relatively independent of each other and can be considered as separate predictors in the model.

Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	Compromise of Confidentiality	.477	2.096
	Compromise of Integrity	.467	2.139
	Compromise Availability	.355	2.819
a. Dependent Variable: ICT system of the Bank			

12 Table: 4.11 Multicollinearity test
Source: Survey result (2023)

7.6. Effect analysis

The effect analysis in this study utilized multiple linear regression to examine the relationship between the independent variables (compromise of confidentiality, compromise of integrity, and compromise of availability) and the banks' business ICT system. The analysis was performed using SPSS version 27, which provided the necessary statistical measurements for the regression analysis.

The main objective of the analysis was to assess the extent to which the independent variables influenced the banks' business ICT system. This was achieved by examining key indicators such as the R-squared value, beta coefficients, and p-values.

The R-squared value indicated the proportion of the variance in the banks' business ICT system that could be explained by the independent variables. A higher R-squared value would suggest a stronger relationship between the independent variables and the dependent variable, indicating that the independent variables have a greater impact on the banks' business ICT system.

The beta coefficients, which were standardized regression coefficients, provided insights into the strength and direction of the relationships between the independent variables and the banks' business ICT system. Positive beta coefficients indicated a positive effect, while negative coefficients implied a negative effect.

The significance of the relationships between the independent variables and the banks' business ICT system was assessed using p-values. A low p-value (typically below 0.05) indicated that the relationship was statistically significant, suggesting that the independent variables had a significant impact on the banks' business ICT system.

By analyzing these measures, the study aimed to determine the magnitude and significance of the relationships between the independent variables and the banks' business ICT system. The results of the analysis would provide valuable insights into the factors influencing the banks' business ICT system in the context of Ethiopia.

7.6.1. Model summary

Model Summary[b]				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.898[a]	.807	.801	.290
a. Predictors: (Constant), Compromise Availability, Compromise of Confidentiality, Compromise of Integrity				
b. Dependent Variable: ICT system of the Bank				

13 Table: 4.12 Model Summary
Source: Survey result (2023)

The model summary results revealed a significant link (R = 0.898) between the independent factors (confidentiality, integrity, and availability) and the dependent variable (the bank's ICT system) at the bank's headquarters. The R-square value was used to assess the goodness of fit, indicating that the explanatory factors effectively described the variations in the dependent variable. The adjusted R-square (R2 = 0.801) indicated that 80.7% of the variation in the bank's ICT system performance and security was explained by the variables of confidentiality, integrity, and availability. The

remaining 19.3% of the issues related to the bank's ICT system were attributed to factors not considered in the study.

7.6.2. Analysis of variance (ANOVA)

ANOVA statistics were employed in the study to assess the goodness of fit of the regression model. ANOVA, a statistical technique used to determine significant differences between groups or samples, was applied to determine the significance of the regression coefficients. If the F-values associated with the independent variables surpass the threshold F-values, it indicates that those variables are significant predictors of the dependent variable. The study's findings are presented in the table below.

ANOVA[a]						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	33.615	3	11.205	133.521	.000[b]
	Residual	8.056	96	.084		
	Total	41.672	99			
a. Dependent Variable: ICT system of the Bank						
b. Predictors: (Constant), Compromise Availability, Compromise of Confidentiality, Compromise of Integrity						

14 Table: 4.13 ANOVA

Source: Survey result (2023)

The findings of the study demonstrate a strong level of statistical significance in the regression model, with a significance level of 0.0%. This indicates that the model is highly effective in predicting the performance and security of a bank's business ICT system based on the variables related to the cyber security triad. The p-value being below the typical threshold of 5% further confirms the model's statistical significance. The adjusted R-square value of 80.7% indicates that the model captures a substantial portion of the variance in the ICT system, highlighting its significant impact. In conclusion, the regression model provides valuable insights into the relationship between the cyber security triad variables and the banks' business ICT system, offering a reliable means of predicting and understanding system performance and security.

7.6.3. Coefficient of determination

The regression coefficient indicates the direction of the relationship between dependent and independent variables. The regression analysis conducted in this study revealed the relationship between the dependent variable, the Bank's business ICT system, and the explanatory factors of the cyber security triad. The regression model, as shown in Table 4.12, is represented by the equation:

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	5.626	0.160		35.208	0.000
	COI	-0.265	0.106	-0.284	-2.499	0.014
	COC	-0.438	0.126	-0.400	-3.488	0.001
	COA	-0.060	0.091	-0.065	-0.658	0.512
a. Dependent Variable: ICT system of the Bank						

15 Table: 4.14 Regression coefficient analysis of the regression model
Source: Survey result (2023)

Y = 5.626- 0.265X1-0.438X2 Where Y= Banks business ICT system
X1= Compromise of Confidentiality
X2= Compromise of Integrity

The coefficients table displays the unstandardized coefficients, standardized coefficients (Beta), t-values, and p-values for each independent variable in the regression model. The constant term (Constant) has a coefficient of 5.626, representing the expected value of the dependent variable when all independent variables are zero. The compromise of confidentiality (COC) variable shows a significant negative relationship with the dependent variable, with a coefficient of -0.265 and a standardized coefficient of -0.284. Similarly, the compromise of integrity (COC) variable has a significant negative impact, with a coefficient of -0.438 and a standardized coefficient of -0.400. However, the compromise of availability (COA) variable does not demonstrate a significant

relationship with the dependent variable, as indicated by its non-significant p-value of 0.512. These coefficients provide insights into the direction, magnitude, and statistical significance of the relationships between the independent variables and the dependent variable, contributing to our understanding of the factors influencing the banks' business ICT system.

The model demonstrates an explanatory power of 80.7%, indicating its ability to account for a significant portion of the variance in the ICT system. The F-statistic for the regression is 133.521, with a p-value of zero.

The results indicate that both the compromise of confidentiality and the compromise of integrity have a statistically significant impact on Ethiopian's private and governmental banks' ICT systems. However, it was found that the compromise of availability does not have a statistically significant impact on the bank's business ICT system.

7.7. Discussion of the regression results

The ultimate objective of the research is to examine the effect of cyber-attacks on banks' business ICT systems in Ethiopia. The regression result showed that there is a strong positive impact of cyber security triads on ICT systems. The research question was addressed based on coefficients of determination ($\mathcal{B}$) and probability values (P). The values of the unstandardized beta coefficients indicate the effects of each independent variable on the dependent variable. Furthermore, the values of the unstandardized beta coefficients in the Beta column of Table 4.12 above indicate which independent variable makes the strongest contribution to explain the dependent variable (bank's business ICT system business operation), when the variance explained by all other independent variables in the model is controlled. Hence using those coefficient results, the proposed research questions for this study were answered as follows.

Q1: Does compromise of confidentiality affect a bank's business ICT systems?

Multiple regression was performed using SPSS to answer the basic research questions. The results showed the overall fitness of the model described in the preceding paragraphs as well as the importance of each independent variable in affecting the dependent variable. The regression analysis revealed that the bank's ICT system is negatively and statistically significantly impacted

by confidentiality (β= -0.438, p = 0.001). The ICT system business operation's performance will decrease by 0.438 units on average if the predictor variable (compromise of confidentiality) goes up by one unit.

Q2: Does a compromise of integrity affect a bank's business ICT system?

Taking into account the national cyber landscape, the compromise of systems or data integrity has a statistically negative significant effect on a bank's business ICT system performance and security, according to the results of multiple regressions shown in Table 4.14 (β= -0.265 and p = 0.014). This suggests that on average, the bank's ICT system performance and security would decrease by 0.265 units if our predictor variable (compromise of integrity) grew by one unit. As a result, the research question is addressed.

Q3: Does compromise of availability affect the bank's ICT system security and operation?

The compromise of the availability of the bank's ICT system during business operations at banks had a statistically insignificant effect on the bank's ICT system, according to the results of multiple regression analysis in Table 4.14 (β = -0.060 and p = 0.512). The researcher is thus able to conclude compromise of availability did not affect the security of the ICT system.

The result of this test goes against the reality or previous findings. The inconveniency of the result might be due to sample size (a larger sample size might support or detect a significant effect of the compromise of availability on the Bank's business ICT system security and performance), the other assumption is that cyber-security experts might rank the CIA triad in context of relativity. i.e., any given financial institution such as banks might choose the compromise of availability over the other compromises. i.e., they might prefer a service outage rather than the compromise of confidentiality and integrity. The other aspect of this finding is its contradiction from the reality in the business perspective, according to the CERT experts most banks prioritize the availability of their system to be one of the major ICT needs because without them their business continuity will be at risk.

In conclusion, as content is an essential variable, it may not always be significant in every context or situation.

Chapter Five

Summary, conclusion, and recommendation

8.1. Summary of major findings

The research aimed to examine the effects of cyber-attacks on banks' business ICT systems in Ethiopia and yielded several significant findings that provide valuable insights into the impact of these attacks.

One key finding was the prevalence of spamming attacks as the most common type of cyber-attack targeting banks' ICT systems, followed by malware attacks. These attacks pose a significant threat to the confidentiality, integrity, and availability of the systems. In particular, Distributed Denial of Service (DDoS) attacks were perceived as having the most severe impact.

The compromise of confidentiality was found to have a negative and statistically significant effect on the bank's ICT system. Breaches in this area can lead to unauthorized access to sensitive data, potentially resulting in financial losses, reputational damage, and legal consequences.

Similarly, the compromise of integrity was identified as a significant concern. When the integrity of the ICT system is compromised, it can affect the accuracy and reliability of data, leading to operational disruptions and potential financial fraud.

On the other hand, the study found that compromise of availability did not have a statistically significant impact on the security of the ICT system. While availability is crucial for uninterrupted operations, it may be prioritized differently by banks compared to confidentiality and integrity. This result was also implied by interviews with stakeholders.

The qualitative analysis highlighted vulnerabilities in banks' business ICT systems, including outdated software, inadequate security measures, insufficient employee training, and poor system maintenance. Addressing these vulnerabilities is essential to strengthen the overall security posture and resilience of the systems.

Cyber-attacks were found to result in significant financial losses for banks. These losses were attributed to various factors such as customer data breaches, operational disruptions, financial fraud, reputational damage, legal expenses, and regulatory fines. Consequently, cyber-attacks can

erode customer trust and damage the reputation of banks, leading to the potential loss of customers and business opportunities.

In conclusion, the research findings underscore the need for banks in Ethiopia to prioritize cybersecurity measures and enhance their resilience against cyber-attacks. It is crucial to invest in robust security measures, regular system updates, employee training, and incident response strategies to mitigate the risks and consequences of cyber-attacks on banks' business ICT systems. By addressing vulnerabilities, protecting confidentiality and integrity, and maintaining customer trust, banks can enhance their security posture and safeguard their operations, reputation, and financial stability.

8.2. Conclusions of the study

The research study aimed to examine the effects of cyber-attacks on banks' business ICT systems in Ethiopia. Through qualitative data analysis, including interviews and document analysis, valuable insights were gained regarding the common types of cyber-attacks, cybersecurity measures, impact on ICT systems, vulnerability management, detection and response capabilities, and collaboration efforts with stakeholders. The findings highlight the urgency for Ethiopian banks to take proactive measures in protecting their digital assets and ensuring the security of customer data.

The study identified phishing attacks, viruses, ransomware attacks, insider threats, and Distributed Denial of Service (DDoS) attacks as common cyber-attack types faced by Ethiopian banks. Continuous monitoring and assessment of vulnerabilities are crucial for strengthening the security posture of banks and effectively mitigating cyber threats.

Ethiopian banks have implemented various cybersecurity measures and protocols, such as firewalls, intrusion prevention systems, and encryption, to establish a robust defense mechanism. However, the persistence of cyber-attacks and challenges in timely detection, resource constraints for effective response, and efficient recovery highlights the need for further research and improvement in incident response mechanisms.

The impact of cyber-attacks on the operations and functioning of ICT systems within banks is significant, leading to financial losses, service disruptions, compromised data, and a decline in public trust. To address these challenges, banks should prioritize incident response planning,

business continuity management, and continuous training and awareness programs for employees. By enhancing their incident response capabilities and strengthening business continuity plans, banks can minimize damage caused by cyber-attacks and ensure the smooth functioning of critical services.

Addressing vulnerabilities and weaknesses is crucial for Ethiopian banks to enhance their cybersecurity practices. Regular vulnerability assessments, penetration testing, and security audits play a vital role in identifying and mitigating potential entry points for cyber attackers. Adopting a proactive risk management approach and promptly addressing vulnerabilities will fortify security controls and reduce the likelihood of successful cyber-attacks.

Advanced detection and response capabilities are essential for Ethiopian banks. Leveraging advanced threat intelligence platforms, deploying intrusion detection systems, and establishing well-defined incident response procedures enable timely detection, effective response, and efficient recovery from cyber-attacks. These measures align with industry best practices and should be prioritized to ensure proactive incident management.

Collaboration with stakeholders is a key aspect of addressing cybersecurity challenges effectively. Ethiopian banks actively participate in information-sharing initiatives, establish public-private partnerships, and contribute to sector-specific working groups. These collaborative efforts facilitate knowledge sharing, exchange of best practices, and coordinated responses to emerging threats. Identifying and addressing potential gaps or limitations in information sharing, increasing participation from stakeholders, and improving coordination in response efforts will foster stronger partnerships.

In conclusion, Ethiopian banks face a dynamic and evolving cyber threat landscape that requires constant vigilance, proactive measures, and collaboration among stakeholders. Investing in cybersecurity capabilities, implementing robust defense mechanisms, and enhancing incident response strategies are crucial. The recommendations provided based on these findings will guide future efforts in improving cybersecurity practices within Ethiopian banks.

8.3. Recommendations

Based on the research findings, the following recommendations are proposed to enhance the cybersecurity practices of Ethiopian banks and mitigate the risks associated with cyber-attacks:

1. **Develop a comprehensive cybersecurity framework**: Ethiopian banks should establish a comprehensive cybersecurity framework that encompasses policies, procedures, and guidelines to address emerging threats and vulnerabilities. This framework should align with international standards and best practices, ensuring a consistent and systematic approach to cybersecurity across the banking sector.
2. **Strengthen collaboration among stakeholders**: Ethiopian banks should foster stronger collaboration with stakeholders, including government agencies, industry associations, and international organizations. This collaboration should focus on information sharing, joint exercises, and coordinated responses to cyber incidents. Regular meetings, workshops, and forums should be organized to facilitate knowledge exchange and promote collective efforts in combating cyber threats.
3. **Enhance employee training and awareness programs**: Banks should invest in regular training and awareness programs to educate employees about the latest cyber threats, attack vectors, and best practices for safeguarding sensitive information. By promoting a culture of cybersecurity awareness, banks can empower their employees to be the first line of defense against cyber-attacks.
4. **Establish a dedicated cybersecurity incident response team**: Ethiopian banks should establish dedicated cybersecurity incident response teams equipped with the necessary skills and resources to detect, respond to, and recover from cyber incidents. These teams should undergo regular training and simulation exercises to ensure their readiness in handling various types of cyber-attacks.
5. **Conduct regular vulnerability assessments and penetration testing**: Banks should perform regular vulnerability assessments and penetration testing to identify and remediate potential weaknesses in their IT infrastructure. These assessments should cover both internal and external systems, including web applications, network infrastructure, and databases. The findings from these assessments should be used to prioritize security investments and strengthen the overall security posture of banks.

6. **Invest in advanced threat intelligence and security analytics**: Banks should leverage advanced threat intelligence platforms and security analytics tools to enhance their detection capabilities. These tools can provide real-time insights into emerging threats and help banks proactively identify and mitigate potential attacks. Continuous monitoring, threat hunting, and anomaly detection should be integral components of the banks' security operations.
7. **Regularly review and update incident response plans**: Banks should review and update their incident response plans regularly to account for changes in the threat landscape and evolving attack techniques. These plans should outline clear roles and responsibilities, communication protocols, and escalation procedures to ensure a swift and coordinated response to cyber incidents.
8. **Conduct periodic security audits and assessments**: Independent security audits should be conducted periodically to evaluate the effectiveness of the banks' cybersecurity measures and identify any gaps or weaknesses. These audits should be performed by qualified external auditors to provide an unbiased assessment of the banks' security controls and practices.
9. **Stay informed about emerging technologies and best practices**: Ethiopian banks should stay abreast of emerging technologies, industry trends, and best cybersecurity practices. Regular participation in industry conferences, seminars, and webinars can help banks gain insights into the latest advancements and adopt relevant technologies and practices to enhance their cybersecurity posture.
10. **Foster a culture of continuous improvement**: Cybersecurity is an ongoing process that requires continuous improvement and adaptation to evolving threats. Ethiopian banks should foster a culture of continuous improvement by regularly reviewing and updating their cybersecurity strategies, engaging in knowledge sharing, and incorporating lessons learned from past incidents into their practices.

By implementing these recommendations, Ethiopian banks can strengthen their cybersecurity defenses, enhance incident response capabilities, and mitigate the risks associated with cyber-attacks. The collective efforts of banks, government agencies, industry associations, and other stakeholders are essential to creating a secure and resilient banking sector in Ethiopia.

8.4. Implication for future research

While this research provides valuable insights into the cyber-attacks faced by Ethiopian banks and the measures implemented to address them, certain limitations should be acknowledged. Firstly, the research focused primarily on quantitative data analysis of a survey study and a qualitative analysis through interviews and document analysis. Future research could benefit from quantitative data analysis of a more sample size survey, and a row data analysis from each bank's CERT teams to provide a more comprehensive understanding of the extent and impact of cyber-attacks in the Ethiopian banking sector.

Secondly, the research was limited to a specific period and hence cross-sectional and may not reflect the current cybersecurity landscape entirely. Given the rapidly evolving nature of cyber threats, ongoing research is essential to stay up-to-date with emerging attack vectors and mitigation strategies.

Lastly, the research was conducted with a specific focus on Ethiopian banks. Future research could expand the scope to include other various financial institutions, such as more microfinance institutions and insurance companies, to gain a broader understanding of the cybersecurity challenges faced by the entire financial sector in Ethiopia.

In conclusion, this research study sheds light on the cyber-attacks faced by Ethiopian banks and provides recommendations to enhance their cybersecurity practices. By implementing these recommendations and addressing the identified limitations, Ethiopian banks can strengthen their cybersecurity defenses and ensure the security of their digital assets and customer data.

REFERENCES

Abraha, H. H., & Hailu, H. (2015). *The State of Cyber Crime Governance in Ethiopia*. Retrieved from http://www.internetlivestats.com/

Acharya, S., & Joshi, S. (2020). *Impact Of Cyber-Attacks on Banking Institutions in India: A Study of Safety Mechanisms and Preventive Measures*. *PJAEE* (Vol. 17).

Adam, A. M. (2020). Sample Size Determination in Survey Research. *Journal of Scientific Research and Reports*, 90–97. doi:10.9734/JSRR/2020/V26I530263

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018, January 1). A Taxonomy of Cyber-Harms Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *Journal of Cybersecurity*. Oxford University Press. doi:10.1093/cybsec/tyy006

Asfaw, T., Advisor, G., & Mulatu, A. (2018). *Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia Addis Ababa, Ethiopia*.

Bachmann, M. (2008). What Makes Them Click? Applying The Rational Choice Perspective To The Hacking Underground. *Electronic Theses and Dissertations*. Retrieved from https://stars.library.ucf.edu/etd/3790

Bezabeh, A. (2015). *Banking Sector Reform in Ethiopia: An Abstract*.

Birru, Y. A. (2019). Ethiopian Financial Sector Development. *The Oxford Handbook of the Ethiopian Economy*, 158–174. doi:10.1093/OXFORDHB/9780198814986.013.9

Bouveret, A., Christo, S., Gaidosch, T., Haksar, V., Kopp, E., Maino, R., … Wiseman, K. (2018). *Cyber Risk for Financial Sectors A Frame Work For Quantitate Assessment*.

Braun amp, C. (2006). *Thematic analysis*. doi:10.1080/08870446.2018.1475670

Brogi, M., Arcuri, M. C., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership and Control*, *15*(2), 70–83. doi:10.22495/cocv15i2art6

Caltagirone, S., Pendergast, A. D., & Betz, C. (2013). The Diamond Model of Intrusion Analysis.

Cambridge. (2017). 2017 Cyber Risk Landscape.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). *CRS Report for Congress The Economic Impact of Cyber-Attacks The Economic Impact of Cyber-Attacks*.

Creswell, J. W., & David Creswell, J. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*.

Debra L. (2002). *Scene of the Cybercrime Computer Forensics Handbook*.

Debra Shinder. (2002). Scene_of_the_Cybercrime_Computer_Forensics_Handbook_Shinder_D_L.

Diogenes, Yuri., & Ozkaya, Erdal. (2018). *Cybersecurity - Attack and Defense Strategies : Infrastructure security with Red Team and Blue Team tactics.* Packt Publishing.

Douglas W. Hubbard. (2016). *How to Measure Anything in Cybersecurity Risk*.

Economic Cost of Cybersecurity. (2020). *Cybersecurity*, 272–303. doi:10.1201/B18335-11

Entrust. (2021). *Banking on Cybersecurity White Paper Best practices to strengthen data security and regulatory compliance in financial services*. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Estimating Cyber Risk for the Financial Sector. (n.d.). Retrieved 30 March 2023, from https://www.imf.org/en/Blogs/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector

Financial intelligence center establishment Regulation no.171/2009 - National Bank. (n.d.). Retrieved 1 April 2023, from https://nbe.gov.et/financial-intelligence-center-establishment-regulation-no-171-2009/

Friis, K., & Ringsmose, J. (n.d.). Conflict in cyberspace : theoretical, strategic and legal perspectives. Retrieved from https://www.worldcat.org/title/945975354

Gerami, M. (2018). *Impact Of Cyber Threats on Business Profitability*.

Global Microscope. (2020). Global Microscope 2020 - Economist Intelligence Unit. Retrieved 21 March 2023, from https://www.eiu.com/n/campaigns/global-microscope-2020/

How NIST's Cybersecurity Framework Protects the CIA Triad. (n.d.). Retrieved 30 March 2023, from https://www.itgovernanceusa.com/blog/how-nist-can-protect-the-cia-triad-including-the-often-overlooked-i-integrity

IBM. (2023). SPSS Statistics | IBM. Retrieved from https://www.ibm.com/products/spss-statistics

Information Network Security Agency. National Information Security Policy, INSA, 2011, 2011 § (2011).

Information Technology Laboratory, COMPUTER SECURITY RESOURCE CENTER, & cyberspace. (n.d.). cyberspace - Glossary | CSRC. Retrieved 31 March 2023, from https://csrc.nist.gov/glossary/term/cyberspace

International Telecommunication Union [ITU]. (2023). Information and communication technologies (ICT) | UNESCO UIS. Retrieved 21 March 2023, from http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict

Kaur, J., & Mustafa, N. (3013). *Examining the Effects of Knowledge, Attitude, and Behaviour on Information Security Awareness: A Case on SME*.

Kott, A., Lange, M., & Ludwig, J. (2018). *Approaches to Modeling the Impact of Cyber Attacks on a Mission*. Retrieved from https://hyrim.net/

Kwadade-Cudjoe, F., Enoch, Y. H., & Bunmi, A. A. (2019). Effect of Cyber Security on Networks Operations (A case study of Vodafone Ghana). *Archives of Business Research*, *7*(6), 16–32. doi:10.14738/abr.76.6589

Leedy, P. D., Ormrod, Jeanne Ellis, A., & Johnson, R. (2017). Practical Research: Planning and Design, 1–20.

Lessa, L., & Negash, S. (2019). *Factors Hindering Full-Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture Integration of ICTs for Sustainable Development View project AMCIS Conference View project*. Retrieved from https://www.researchgate.net/publication/336133371

Li, H. E. (2017). *Three Essays on Cyber Security Issues*.

Manivannan, A., & Moorthy, D. (2020). Cyber Attacks in The Banking Industry. doi:10.13140/RG.2.2.16664.01282

Musman, S., Temin, A., Tanner, M., Fox, D., & Pridemore, B. (2008). *Evaluating the Impact of Cyber Attacks on Missions*.

NBE. (2021). National Bank of Ethiopia Annual Report, NBE, 2021-22. doi:10.5-13.5

Neuman, W. L. (2014). *Social Research Methods Qualitative and Quantitative Approaches (7th ed.). Essex Pearson. - References - Scientific Research Publishing*. *2014*. Retrieved from https://www.scirp.org/(S(oyulxb452alnt1aej1nfow45))/reference/ReferencesPapers.aspx?ReferenceID=2061116

Okeshola, F. B., & Adeta, A. K. (2013). *The Nature, Causes, and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria*. *American International Journal of Contemporary Research* (Vol. 3). Retrieved from www.aijcrnet.com

Paul Bocij; Andrew Greasley; Simon Hickie. (2020). Business information systems, Third edition. Retrieved from https://www.worldcat.org/title/1117709106

PWC. (2014). Threats to The Financial Services Sector.

Raghavan. (2014). *The Effect of Cybercrime on A Bank's Finances*. Retrieved from www.ijcrar.com

Rao, H. S. (2019). Cyber Crime in Banking Sector. *International Journal of Research-Granthaalayah*, *7*(1), 148–161. doi:10.5281/zenodo.2550185

Simple Overview of CMMC and NIST 800-171: Ready, Set, Go! (n.d.). Retrieved 30 March 2023, from https://adeliarisk.com/cmmc-vs-nist-800-171/

Stanikzai, A. Q., & Shah, M. A. (2021). *Evaluation of Cyber Security Threats in Banking Systems*. In *2021 IEEE Symposium Series on Computational Intelligence, SSCI 2021 - Proceedings*. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/SSCI50451.2021.9659862

Tariq, N. (2018). *Journal of Internet Banking and Commerce IMPACT OF CYBER ATTACKS ON FINANCIAL INSTITUTIONS*. *Journal of Internet Banking and Commerce* (Vol. 23). Retrieved from http://www.icommercecentral.com

Temesgen, A. (2022). *Cyber-Attack Vulnerability and Its Implication Towards Digital Economic Development in Ethiopia*.

The CIA Triad and Real-World Examples. (n.d.). Retrieved 30 March 2023, from https://blog.netwrix.com/2019/03/26/the-cia-triad-and-its-real-world-application/

The CIA triad: Definition, components, and examples | CSO Online. (n.d.). Retrieved 30 March 2023, from https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

These are the top cybersecurity challenges of 2021 | World Economic Forum. (n.d.). Retrieved 31 March 2023, from https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

Triki, T., & Faye, I. (2013a). *Financial Inclusion in Africa*.

Triki, T., & Faye, I. (2013b). *Financial Inclusion in Africa*.

Tsion Mathewos. (2015). *Cybercrime On Internet Banking Activities in Ethiopia*.

Uma Sekaran. (2006). *Research Methods For Business: A Skill Building Approach, 4Th Ed - Uma Sekaran*. Retrieved from https://books.google.com.et/books/about/Research_Methods_For_Business_A_Skill_Bu.html?id=4kEjysnZQTkC&redir_esc=y

UN. (2023). Developments in the field of information and telecommunications in the context of international security – UNODA. Retrieved 1 April 2023, from https://www.un.org/disarmament/ict-security/
Using the CIA Triad to Boost Cyber Resilience - WSJ. (n.d.). Retrieved 30 March 2023, from https://deloitte.wsj.com/articles/using-the-cia-triad-to-boostcyber-resilience-1542679329
Von Solms, S. H., & Von Solms, R. (2009). Information security governance. *Information Security Governance*, 1–134. doi:10.1007/978-0-387-79984-1
Woretaw, A., & Lessa, L. (2012). *Information Security Culture in The Banking Sector in Ethiopia*.
Worku, G. (2010). *Electronic-Banking in Ethiopia-Practices, Opportunities and Challenges*. Retrieved from http://ssrn.com/abstract=1492006Electroniccopyavailableat:http://ssrn.com/abstract=1492006

Appendix

Appendix A: Survey questioner

St. Mary's University

School of Business
Department of Business Administration

Dear respondents;

Thank you for taking the time to participate in this questionnaire. Your input is crucial for the study on the effect of cyber-attacks on banks in Ethiopia. Your honest and sincere responses to the questions will help us better understand the challenges and risks that banks face concerning cyber-attacks. Please rest assured that all information provided will be kept strictly confidential and used solely for academic purposes. Once again, I appreciate your cooperation and willingness to contribute to this important research.

Thank you.

Directions for filling out the questionnaires

- Do not write your name
- Select or mark in the button provided for choice questions

Bisrat Aimero

Tel: +251911484437
E-mail: bisrataimero@gmail.com

Section A: Demographic Information about Respondents

1) What is your gender?

□ Male □ Female

2) What is your age?

□ 20-30 □ 31-40 □ 41-50 □ Above 50

3) What is your highest level of education completed?

□ Diploma □ Degree. □ Masters □ PHD

4) What is your current profession?

□ Network or IT Administrator / Engineer
□ SOC / CERT Administrator / Analyst
□ Developer (Web, Cloud, software)
□ Cyber security (Penetration tester, Analyst, or Auditor)
□ Team Leader / Manager
□ Business / Finance

5) Which industry are you currently working on?

□ Private Banking Sector
□ Government banking Sector
□ Microfinance Institutions
□ Government Security Institutions (INSA.)

6) How many years of experience do you have?

□ 0-5 □ 6-10 □ 11-15 □ Above 15

Section B: Technical Questionnaire for Professionals

1) Please indicate all of the cyber security incidents (cybercrime) committed against your organization and the frequency with which they occur by indicating the numbers as 1= Never, 2= Rarely, 3=Occasionally 4=Frequently and 5=Always

	Variable	**Scale Measurement**				
	Type of Cyber-attacks	1	2	3	4	5
1)	Phishing attack					
2)	Distributed denial of service (DDOS) attack					
3)	Ransomware attack					
4)	Web-based attack (SQL injection, Cross-Site Scripting (XSS) attacks defacement					
5)	Malware attack					
6)	Spamming					

2) What is the level of importance for the following bank's ICT systems necessary for business operations (Indicate the levels of business criticality for the following ICT systems.)? Rate their level of importance according to the questions by as by selecting the numbers 1= Never, 2= Rarely,3=Occasionally4=Frequently and 5=Always

	Variable	**Scale Measurement**				
	ICT systems of Banks	1	2	3	4	5
1)	Core banking systems are the most important ICT systems in the bank					
2)	Mobile banking applications are the most important ICT systems in the bank					
3)	Data centers, storage, and servers are the most important ICT systems in the bank					
4)	Security appliances (Firewalls, IPS, IDS, antivirus, and antimalware) are the most important ICT systems in the bank					
5)	Electronic payment systems (such as NEFT, RTGS, and UPI) are the most important ICT systems in the bank					

3) Please indicate the severity (damaging) level for each type of cyber-attack if they are successfully executed on the bank's business-critical IT systems accordingly as 1= Not severe, 2=Slightly severe, 3=Moderately severe, 4=Very severe, and 5=Extremely severe

	Variable	**Scale Measurement**				
	Type of Cyber-attacks	1	2	3	4	5
1)	Phishing attack					
2)	Distributed denial of service (DDOS) attack					
3)	Ransomware attack					
4)	Web-based attack (SQL injection, Cross-Site Scripting (XSS) attacks defacement					
5)	Malware attack					
6)	Spamming					

4) Compromise of Confidentiality: Indicate your level of agreement for the measure of the degree of compromise of confidentiality according to the statement as 1= Strongly disagree, 2=Disagree, 3= Neutral, 4= Agree, and 5=Strongly agree

	Variable	**Scale Measurement**				
	Compromise of Confidentiality:	1	2	3	4	5
1)	The compromise of confidentiality has a significant negative impact on the security of customer information, even in the event of a cyber-attack.					
2)	The banks' measures to protect customer data from unauthorized access or disclosure are not fully effective against cyber-attacks.					
3)	The compromise of confidentiality due to cyber-attacks undermines the effectiveness of the banks' measures to ensure data security.					
4)	Cyber-attacks significantly impact the confidentiality of customer transactions within the banks' systems.					
5)	The banks frequently encounter cyber-attack problems affecting the confidentiality of their business ICT systems.					
6)	Customer trust in the banks' ability to safeguard their confidential information is compromised by cyber-attacks.					

5) Compromise of Integrity: Indicate your level of agreement for the measure of the degree of compromise of integrity according to the statement as 1= Strongly disagree, 2=Disagree, 3= Neutral, 4= Agree, and 5=Strongly agree

	Variable	**Scale Measurement**				
	Compromise of Integrity:	1	2	3	4	5
1)	The accuracy and reliability of transactional data are compromised by cyber-attacks during transactions.					
2)	Cyber-attacks significantly compromise the integrity of data stored in the bank's systems for online banking.					
3)	The bank's systems fail to effectively prevent unauthorized alteration or manipulation of data during cyber-attacks.					
4)	Cyber-attacks undermine the trustworthiness and reliability of the bank's data.					
5)	The bank's data integrity for mobile applications is vulnerable to user-side cyber-attacks.					
6)	Customer confidence in the accuracy and integrity of the bank's data is negatively impacted by cyber-attacks.					

6) Compromise of Availability: Compromise of Integrity: Indicate your level of agreement for the measure of the degree of compromise of integrity according to the statement as 1= Strongly disagree, 2=Disagree, 3= Neutral, 4= Agree and 5=Strongly agree

	Variable	**Scale Measurement**				
	Compromise of Availability	1	2	3	4	5
1.	Mobile banking services are frequently disrupted and become non-functional during cyber-attacks.					
2.	The bank's online services experience significant disruptions and unavailability during a DDoS attack.					
3.	Cyber-attacks frequently cause disruptions and unavailability of critical banking services.					
4.	The bank struggles to maintain uninterrupted access to its services in the face of cyber-attacks.					
5.	The availability of online banking services is severely compromised by cyber-attacks.					
6.	Customer convenience and access to banking services are significantly impacted by cyber-attacks.					

Thank You!

Appendix B: Interview questions

1. In your experience, what are the most common types of cyber-attacks that banks' business ICT systems encounter, and how do these attacks impact their overall security?
2. Can you share specific instances where the confidentiality of sensitive customer information was compromised due to a cyber-attack on a bank's ICT systems, and what were the consequences of these breaches?
3. How do cyber-attacks typically compromise the integrity of banks' business ICT systems, and what potential risks or consequences arise from unauthorized modifications or alterations to critical financial data?
4. What are the common techniques cyber attackers use to disrupt the availability of banks' business ICT systems, and how do these attacks impact the continuity of banking services?
5. Can you provide examples of successful exploitation of vulnerabilities during penetration testing that resulted in compromising the availability of banks' ICT systems, and what countermeasures should banks implement to mitigate these risks?

ቅድስት ማርያም ዩኒቨርሲቲ
ድኅረ-ምረቃ ት/ቤት

St. Mary's University
School of Graduate Studies

☎+251-11-552-45 03 ✉1211, 18490 Fax 011552 83 49 e-mails: sgs@smuc.edu.et, Addis Ababa, Ethiopia

Ref. No.: SGS/2196/2023

Date: May 16/ 2023

TO : Information Network Security Administration (INSA)

Addis Ababa

Subject: Request for Cooperation

Bisrat Aimero ID No. SGS/0033/2013B is a post graduate student in the **Department of Masters of Business Administration (MBA).** He is working on his Thesis entitled **"The Effect of Cyber Attack on Banks Business ICT Systems: The Case of Selected Banks in Ethiopia,"** and would like to collect data from your institution.

Therefore, I kindly request your good office to allow him to access the data he needs for his research.

Any assistance rendered to him is highly appreciated.

Sincerely,

Samuel Fantaye Tessema
Guidance Counselor and Thesis Coordinator

የኢንፎርሜሽን መረብ ደህንነት አስተዳደር
የሰነድ ማደራጀ እና አስተዳደር
ደብዳቤው የደረሰበት ቀን 11/9/15
የደብዳቤው ቁጥር ጠሀፃ 16/2023
የማህደር ቁጥር 3611