A Cyber Insurance Framework for Ethiopia: Key Components and Recommendations

Ephrem Baheru Assefa

Advisor: Sileshi Demesie (PhD)

School of Information Technology and Engineering (SiTE)

Addis Ababa Institute of Technology

Addis Ababa University

November 2024

A Cyber Insurance Framework for Ethiopia: Key Components and Recommendations

Name and signature of Members of the Graduate Examining Committee

	Signature	Date
Sileshi Demesie (PhD) **Research Advisor**	----------	----------
Dr. ---------- **Examiner**	----------	----------
Dr. ---------- **Examiner**	----------	----------

Authors declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted as a candidature for any degree in any university.

I declare that the thesis is a result of my investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor, Sileshi Demesie (PhD). Other sources are acknowledged by proper citations, giving explicit references. A list of references is appended.

Signature: _____

Ephrem Baheru

This thesis has been submitted for examination with my approval as university advisor.

Advisor's Signature: _____

Sileshi Demesie (PhD)

Acknowledgement

I am profoundly grateful to the Almighty GOD for bestowing me the strength, patience, and determination required to complete this thesis.

My appreciation goes to my advisor, Sileshi Demesie (PhD), whose unwavering support, patience, motivation, and extensive knowledge have been invaluable. His insightful guidance has been instrumental in the research and writing of this thesis.

I extend my sincere thanks to my classmates, friends and colleagues. The spirit of camaraderie we shared over the years, and our fruitful discussions have significantly enriched my learning experience.

I owe a debt of gratitude to my entire family for their untiring spiritual support throughout the process of writing this thesis and in all aspects of my life.

The completion of this thesis has been made possible through the blessings of the Almighty and the support of everyone mentioned above.

Abstract

The exponential rise in cyber threats such as ransomware, identity theft, and other forms of cybercrime has driven many organizations to seek cyber insurance as an extra layer of protection. Cyber insurance has emerged as a means of mitigating residual risks that remain after implementing various cyber risk mitigation strategies. Cyber-attacks in Ethiopia have been rising steadily each year, driven by a surge in digital transformation initiatives across various sectors, including government, financial institutes, and other critical infrastructure. This highlights the urgent need for cyber insurance services in the country, as it could help organizations manage financial losses and recover more effectively from cyber incidents. This study reveals that no insurance provider in the country currently offers cyber insurance services. This research envisioned promoting cyber insurance practice in Ethiopia by developing a cyber insurance framework that could be used by public and private organizations. To develop the framework, data was collected through a face-to-face interview with insurers, potential insureds, and regulatory bodies, and the data was analyzed using a qualitative approach. We also studied global best practices and trends in cyber insurance. The framework is designed to help Ethiopian organizations manage cyber risks and effectively recover from cyber incidents and reputational damage. The framework includes key components such as stakeholder engagement, insurance coverage, risk assessment and underwriting, premium calculation, risk mitigation and loss prevention, incident response and claims process, regulatory compliance, awareness and education, review and iteration, collaboration, and information sharing. A case study is used to demonstrate how a company successfully implemented the cybersecurity framework.

Key words: Cyber Insurance, Cyber risks, Cyber security, Decision makers

Table of Contents

Abstract v

List of Figures ix

List of Tables x

List of Acronyms and Abbreviations xi

CHAPTER ONE 1

Introduction 1

1.1. Statement of Problem 2

1.2. Research Questions 3

1.3. Objective of the Study 3

1.3.1. General Objective 3

1.3.2. Specific Objective 3

1.4. Contribution of the Thesis Study 4

1.5. Scope/Delimitation 4

1.6. Document organization 5

CHAPTER TWO 7

Literature Review 7

2.1. Introduction 7

2.2. Digital Transformation 7

2.3. Cybersecurity Landscape in Ethiopia 10

2.4. Insurance in Ethiopia 11

2.5. Cyber Insurance 12

2.5.1. Evolution of Cyber Insurance 12

2.5.2. Cyber insurance market 13

2.5.3. Legal and Regulatory frameworks 16

2.6. Related Works 17

2.6.1. Gap Analysis 18

CHAPTER THREE 21

Research Methodology 21

3.1. Introduction 21

3.2. Research Approach 21

3.3. Research Design 22

3.4. Data Collection Methods 23

3.5. Population and Sample 24
3.5.1. Population 24
3.5.2. Sample and Sampling method 24
3.6. The Research Instrument 25
3.7. Data Analysis 25
3.8. Limitations of the study 25
3.9. Demographic Data of the respondents 26
3.10. Ethical Considerations 26
CHAPTER FOUR 27
Analysis and Discussion 27
4.1. Introduction 27
4.2. Thematic Analysis 27
4.2.1. Ensuring Compliance and Standards 27
4.2.1.1. Understanding Regulatory compliance 27
4.2.1.2. Navigating International Standards and Frameworks 28
4.2.1.3. Accredited Certifiers 28
4.2.1.4. Mandatory Requirements 28
4.2.2. Identifying Risks and Ensuring Resilience 28
4.2.2.1. Understanding risks 28
4.2.2.2. Risk Assessment 29
4.2.2.3. Risk Management Frameworks 29
4.2.2.4. Threats and Threat levels 29
4.2.2.5. Proactive risk mitigation 30
4.2.3. Cyber Insurance and Coverage Challenges 30
4.2.3.1. Cyber insurance explanation 30
4.2.3.2. Components of Cyber Insurance Policies 30
4.2.3.3. Challenges and Gaps in Cyber Insurance 30
4.2.4. Lack of trust, information hiding, lack of clarity 31
4.3. Cyber Insurance Framework Synthesization 32
4.3.1. Synthesizing RQ 1 37
4.3.2. Synthesizing RQ 2 39
4.3.3. Synthesizing RQ 3 42
4.4. Discussion 43

CHAPTER FIVE 46
Proposed Cyber Insurance Framework 46
5.1. Introduction 46
5.2. Component Description 46
5.3. Case Study 56
Introduction 56
Step one – Request Form 57
Step two – Application Review 57
Step three – Document and Physical Evaluation 58
Step four – Third-party Evaluation 59
Step five – policy providing 59
CHAPTER SIX 60
Summary and Future work 60
6.1. Summary 60
6.2. Recommendations and Future work 61
REFERENCES 62
APPENDICES 66
Appendix - A Baseline Assessment 66
Appendix - B Interview Question 1 69
Appendix - C Interview Question 2 71
Appendix – D Interview Question 3 72

List of Figures

Figure 1:Ethiopian Cybersecurity Commitment (Source: (ITU, 2024)) 11
Figure 2.Research Approach 22
Figure 3. Research Design Summary 23
Figure 4. Cyber insurance Framework architecture 46
Figure 5. Engaged parties of risk assessment and underwriting component 50
Figure 6. Documents and Physical evaluation 58
Figure 7. Summary of Case Study 59
Figure 8. Steps performed by cyber insurance policy holder 68

List of Tables

Table 1. Summary of gap analysis 18
Table 2:Summarized list of participants 25
Table 3:Summary of participant's profile 26
Table 4:Synthesization matrix 32
Table 5:Rating loss severity 69

List of Acronyms and Abbreviations

AIG – American International Group

ATM – Automated Teller Machine

CISO – Chief Information Security Officer

CRAM – Cyber Risk Assessment and Mitigation

DFS – Department of Financial Services

ETB – Ethiopian Birr

EU – European Union

GCI – Global Cybersecurity Index

GDPR – General Data Protection Regulation

GNI – Gross National Income

GOE – Government of Ethiopia

ICT – Information and Communication Technology

ITU – International Telecommunication Union

LDCs – Least Developed Countries

SMEs- Small and Medium Enterprises

UK – United Kingdom

U.S.A – United States of Amer

CHAPTER ONE

Introduction

The exponential growth of cyber-attacks around the globe is a major cyber risk to all countries and organizations. According to (World Economic Forum Accenture, 2022), there are numerous cyber challenges that affect the cyber domain as a key finding. Organizations perform cyber risk assessments to identify potential cyber threats that could affect or disrupt the organization's day-to-day business operations. Among different risk mitigating techniques, transferring risk to a third party is a relatively new trend globally (Bodin et al., 2018). This risk-transfer strategy is implemented by purchasing cyber insurance premiums from insurance companies.

The growing awareness of the expanding cyber-attack surface area, growing dependencies on technology, and the complex cyber threat landscape are all contributing to the increasing demand for cyber insurance (IAIS, 2019). The largest cyber-attack occurrence to date was NotPetya which occurred in 2017, resulting in an estimated $10 billion in losses, $3 billion of which was reimbursed by the insurance industry (IAIS, 2019). According to the Allianz Risk Barometer 2023 report (Article, n.d.), cyber incidents are ranked top with 34%. This position indicates the importance of today's digital economy, the expanding threat of ransomware and extortion, and geopolitical rivalries and conflicts that are increasingly being played out in cyberspace. The share of cyber insurance in the entire industry is minimal compared to the property and casualty premium pool. However, cyber insurance is the fastest-growing new line in the insurance industry (Petrović, 2020). Cyber insurance typically focuses on the less uncertain risks or constrains uninsurable risks to make them more manageable (Petrović, 2020).

Since cyber insurance is a new component and different from traditional insurance approaches, it has unique parameters for setting the insurance premium, which is not found in other insurance rates (Aziz et al., 2020). The concept and market for cyber insurance are still in their infancy stage. Many business managers are unfamiliar with this cyber risk mitigation technique. Business leaders and industry experts might not be aware of this new trend in their respective business sectors (IAIS, 2019; Woods & Simpson, 2017).

Implementing cyber insurance is an unavoidable priority in our country's current circumstances, although there is a lack of regulatory policies and cyber insurance laws regarding cyber insurance (Granato & Polacek, 2019).

1.1. Statement of Problem

According to (Gebremeskel et al. 2023), Ethiopia's digital transformation has progressed considerably as the business environment has grown more dynamic. The authors highlighted that digital transformation has helped firms improve organizational agility, stakeholder participation, transparency, and networking. As a result, Ethiopia has seen an increase in cyber-attacks year after year.

In 2013, there were 59 registered attacks. According to the most recent bi-annual report delivered by INSA, 4,623 cyber-attacks were documented in the first half of 2024. According to the report, the attack volume has increased by 115%, and those attacks would have resulted in damage of nearly 10.5 billion Birr. Both governmental and non-governmental organizations have been affected by these attacks. The report confirms that critical infrastructure, including telecom, financial institutions, power, and Ethiopian Airlines, were major targets.

The state-owned Commercial Bank of Ethiopia (CBE) reported that the bank has been a primary target of groups seeking to harm Ethiopia for political and economic reasons. CBE reported that it successfully thwarted approximately 28,000 cyber-attacks since 2022. On March 16, 2024, a cyber incident occurred, which led the bank clients to withdraw a large sum of money from the bank's ATM and transfer millions of Birr digitally. The bank described this event as a "system glitch" rather than a cyber-attack, according to Reporters, 2024.

As cyber incidents become more sophisticated and frequent, there is a need for a cyber insurance framework to help manage residual risks. As per our knowledge, currently, there are no insurance companies that provide cyber insurance services in the country. Therefore, developing a framework that could be used to practice cyber insurance to provide financial protection against any losses caused by cyber incidents is critical.

A number of researchers have studied cyber insurance from diverse perspectives. For instance, the availability and readiness of cyber insurance policies were assessed by (Makanda & Kim, 2017). A market analysis of cyber insurance was conducted by (Pavel, 2020) and (Abd Rahman et al., 2022). Meanwhile, (Schwieger & Ladwig, 2022) argued that academics should pay greater attention to integrating cyber insurance into business curricula. Other scholars, such as (Wang, 2019) and (Mukhopadhyay et al., 2019), suggested frameworks focusing on information security investment and cyber risk management/mitigation, respectively. Building on these insights, in this research, we aim to propose a framework that offers a comprehensive solution to practice cybersecurity insurance tailored to Ethiopia's cybersecurity landscape.

1.2. Research Questions

The following questions are addressed in this research study;

1. What are the legal and regulatory frameworks related to cyber insurance in Ethiopia, and their impact on the feasibility of cyber insurance?
2. To what extent are organizations aware of cyber insurance practices, and how do they perceive the necessity and feasibility of implementing a cyber insurance framework to manage cyber risk?
3. What are the current trends and best practices on cyber insurance?
4. What are the key components of a cyber insurance framework, and how can they be used to effectively manage cyber risks?

1.3. Objective of the Study

1.3.1. General Objective

The research aims to explore the legal, regulatory, and practical aspects of cyber insurance in Ethiopia and develop a cyber insurance framework for Ethiopian organizations.

1.3.2. Specific Objective

The specific objectives of this research are presented below.

- Identify and analyze the existing legal and regulatory frameworks related to cyber insurance in Ethiopia.

- Evaluate how these frameworks influence the feasibility and implementation of cyber insurance products.
- Assess the current practices of cyber insurance in Ethiopia.
- Measure the level of awareness among organizations regarding cyber insurance practices.
- Explore organizational perceptions of the necessity and feasibility of a cyber insurance framework for managing cyber risks.
- Identify the key components of an effective cyber insurance framework.
- Develop a comprehensive Cyber Insurance Framework for Ethiopian public and private organizations.
- Evaluate how this framework can be leveraged to manage cyber risks effectively within organizations.

1.4. Contribution of the Thesis Study

By analyzing the best practices and current trends in both the insurance and cybersecurity industries, this research has contributed to a comprehensive cyber insurance framework for Ethiopian organizations. To the best of our knowledge, this work is the first to indicate or propose introducing a cyber insurance coverage policy in our country.

1.5. Scope/Delimitation

The study will focus on developing a cyber insurance framework for use by Ethiopian insurance companies. The study sought to gather perspectives from insurers and insured parties' regarding the cyber insurance policy offered by the insurer using this framework.

This study identifies limitations due to the complexities of cyber insurance and the methodology employed in the investigation. One key problem is determining cyber insurance premiums, which are determined by a variety of criteria, such as the organization's size, industry, and previous cyber occurrences. Inaccurate or partial data may impede the development of a uniform method for premium calculation. Furthermore, the ever-changing nature of cyber threats and a lack of comprehensive frameworks for analyzing these risks limit the efficiency of risk assessments. The use of subjective

judgments in determining organizational vulnerabilities can make risk estimates less accurate.

Furthermore, the study has limitations in the areas of forensic assessment and cyber risk modelling. Forensic investigations are frequently difficult and time-consuming, and the results can vary greatly depending on the methodology used. This unpredictability has the potential to influence the consistency and credibility of cyber risk estimation estimates. Furthermore, conventional approaches for evaluating cyber risks may fail to capture the full range of potential losses, especially in the face of new threats and vulnerabilities. These limitations underscore the need for more robust, standardized approaches to cyber insurance that use precise risk assessment and quantification tools to improve decision-making in this continuously changing world.

1.6. Document organization

The rest of the thesis is structured as follows:

The second chapter explains the current condition of insurance in Ethiopia, followed by a discussion of the literature on several themes, such as digital transformation, Ethiopia's cybersecurity landscape, and cyber insurance. The cyber insurance issue covers various topics that are both directly and indirectly related to cyber insurance, such as the evolution of cyber insurance, the current cyber insurance market, laws, and dangers. This section of the paper includes references to related publications by other scholars.

Chapter three explains the technique, including the research strategy and its arrangement. The chapter also addressed the research design, data collection methodologies, population, and sampling. It also mentioned how the acquired data was examined. Furthermore, the chapter summarizes the study limitations, the respondents' demographic data, and ethical considerations.

The fourth chapter comprehensively analyzed and discussed Ethiopia's present cyber insurance practices. The chapter provided a thorough summary of the interview questions responses obtained from important stakeholders and potential cyber insurance policy users.

The fifth chapter of the paper describes the main contribution of the research work presented. This study proposes a cyber insurance framework for Ethiopian institutions as a means of transferring residual cyber risks. The framework comprises ten components that are explored in length; nevertheless, the framework's feasibility is also demonstrated as a case study in this chapter.

The discussion part of the thesis is also addressed in this section of the document. The rest of the document presents the summary and future work, as well as references and appendices, which contain the interview questions that are in use for the data collection.

CHAPTER TWO

Literature Review

2.1. Introduction

This chapter reviews the literature released by various scholars. The literature navigates cyber insurance from different perspectives. This chapter of the document discusses Ethiopia's digital transformation strategy, which is set and intended for completion by 2025. It also provides insight into cyber insurance, including a brief history and other important aspects of cyber insurance practices and other components. The current cyber security landscape of Ethiopia is addressed in this chapter. The chapter also contains related works that may be used to show the importance of this work. The gaps between the related works and the original point of view of this work are presented here.

2.2. Digital Transformation

In their work, Ebert et al.(Ebert & Duarte, 2018) defined Digital transformation as simply adopting disruptive technologies to increase productivity, value creation, and social welfare. Digital transformation may be produced by many nations, multilateral organizations, and industry associations to show their strategic foresight studies and ground their long-term policies. The authors mentioned that data analytics, cloud storage and services, convergent interactivity and cognition, augmented reality with visualization and simulation, pattern recognition, machine learning, and AI are facilitating a convergence of IT and embedded systems. In this regard, the authors clearly show that digital transformation is opening the doors for technological innovation, new business models, and cross-industry collaboration.

A report by GSMA focusing on Ethiopia, published in October 2024, highlights that policymakers have identified key objectives to accelerate economic growth through digitization. Digitalization serves as a catalyst for both economic expansion and socio-economic development, with the mobile telecommunications industry and mobile money playing a central role in this transformation.

In Ethiopia, digitalization is progressing steadily, with mobile telecommunications networks increasingly supporting the availability and usage of digital services. The widespread adoption of digital technologies in both the public and private sectors is fostering better interactions between individuals, enabling more efficient resource use, enhancing productivity, and driving innovation.

In its policy brief, the author (Director, 2022) states that Simple mobile phones enable African households to access information, conduct business, receive money, and use mobile devices for innovative applications such as healthcare and education. It was primarily these transactional implementations of digital innovations and the availability of access to mobile devices that fed the hype and unrealistic expectations of what can be accomplished with digital technology and the possibility of developing countries leapfrogging. The assumption is that in an unregulated and free market system, the rapid pace of penetration will allow emerging countries to attain inclusive growth and transform their economies to catch up with rising or advanced economies.

Ethiopia's Information and Communication Technology (ICT) landscape is rapidly evolving. Currently, the communication sector contributes about 2% to the country's GDP, compared to an average of 4% in the East African region[1].

To support the transformation, the GOE has developed several major digital portals, including ones for e-trade, e-procurement, e-service, a city portal, and ease-of-doing-business portals. These platforms are to assist in the country's development in the coming years. Through these portals, the government has digitized more than 130 services across 25 service providers, including authorities, ministries, agencies, and other government institutions.

Since 2020, there has been significant growth in the number of data centers built in Ethiopia. The GOE has also developed a dedicated IT Park 18 miles outside Addis Ababa in Bole Lemi, designed to attract companies that outsource ICT services as well as those involved in manufacturing and exporting IT equipment. Raxio, the first Tier III certified data center, began operations in November 2022. Other private sectors investors, such as

[1] https://www.trade.gov/country-commercial-guides/ethiopia-digital-economy

Wingo Africa and Redfox Solution Group, are also investing in data center development in Ethiopia. Additionally, government institutions have made considerable investments in data centers.

According to Ethio Telecom data, internet users in Ethiopia have reached 40.4 million. The density of fixed and mobile voice subscribers has reached 821 thousand and 75.6 million, respectively. Both Ethio Telecom and Safaricom are actively investing in expanding their telecommunications infrastructure. Ethio Telecom completed its infrastructure expansion under the Expansion Telephone Plan I (ETP I), partnering with China's ZTE, Huawei, and the Swedish firm Ericsson. This expansion focuses on providing telecom services to all 15,000 rural villages in Ethiopia, with dedicated lines for agriculture, education, health, and consumer use.

The GOE is also actively developing directives that help the Mobile Money Regulatory Index and Interoperability of systems, and other regulatory frameworks that facilitate digitalization like the Electronic Transactions Proclamation, which creates provisions for consumer protection, digital payments, digital signatures, and electronic receipts.

Eth switch presented at the Ethiopia Digital Payment Conference, which NBE prepared on 06 April 2024, that the national payment initiative plays a crucial role in modernizing the payment ecosystem. After the establishment of Eth switch, the payment ecosystem's interoperability ensures seamless transactions, allowing payments to and from anyone using a unified account and standardized payment tools, irrespective of the service provider[2].

Ethio Telecom changed Ethiopia's financial landscape by launching its Telebirr mobile money product in 2021, moving the country away from a predominantly cash-based system. Developed in collaboration with Dashen Bank, Telebirr is an online payment and money transfer application that allows users to deposit cash, send money, receive payments, and withdraw cash. Users can also use Telebirr to buy airtime and packages, pay for utilities and traffic fines, and make payments to merchants. Since its launch,

[2] https://nbe.gov.et/wp-content/uploads/2024/04/3.Presentation_1_AL.pdf

Telebirr has gained 41 million subscribers and facilitated transactions worth 910.7 billion Ethiopian Birr (ETB).

Ethiopia's digital financial services sector is poised for further change with the introduction of Safaricom's m-Pesa in August 2023, a well-established product in the Kenyan market. As of January 2024, Safaricom had signed up 3.1 million users for m-Pesa in Ethiopia. It is hoped that other players will be able to enter the market as the countries continues steps to liberalize the banking and finance sector.

The pending launch of Ethiopia's first capital market and securities exchange indicates the need for the government to develop the economy by creating a modern and efficient trading system. This helps to attract modern digital infrastructure, electronic trading platforms, and order management systems into the country.

2.3. Cybersecurity Landscape in Ethiopia

The author (Adane, 2022) summarized different researchers' points of view regarding the country's cyber security landscape. In his work, the author criticizes the researchers' contribution. He believes that the findings provided by INSA regarding risks to the country's critical infrastructure should be addressed by developing a standardized legal framework and by promoting institutions to utilize recognized cybersecurity frameworks. The author also put emphasis on tackling the lack of cybersecurity expertise and awareness of cyber-attacks by developing and delivering virtual training systems or intelligent tutoring systems.

Aschenek, in his work (Aschenek Zeleke, 2019), mentioned the sluggishness of the internet and lack of access which are results of insufficient governance capability. The author emphasizes the importance of digital sovereignty in today's world. The author also mentioned that there was excessive control of the digital landscape. Those controls, according to the author, create restrictions on access to information. He also argues that the legal and policy environment should be shaped to limit the full utilization of digital opportunities rather than creating a conducive environment.

In this edition (ITU, 2024), ITU explores member states' level of cyber security commitment. The GCI report employs five levels of tiers to analyze countries' cybersecurity commitments using the pillars: legal, technical, organizational, capacity development and cooperation. Based on the pillars mentioned above, Ethiopia scores a little higher than the average score of the African region. According to the evaluation, Ethiopia's cybersecurity commitment is relatively strong in terms of legal measures, capacity measures, and organization measures. Technical and organizational measures have been recognized as areas of potential growth. Ethiopia was categorized as establishing stage on tier performance based on the result evaluated out of 20.

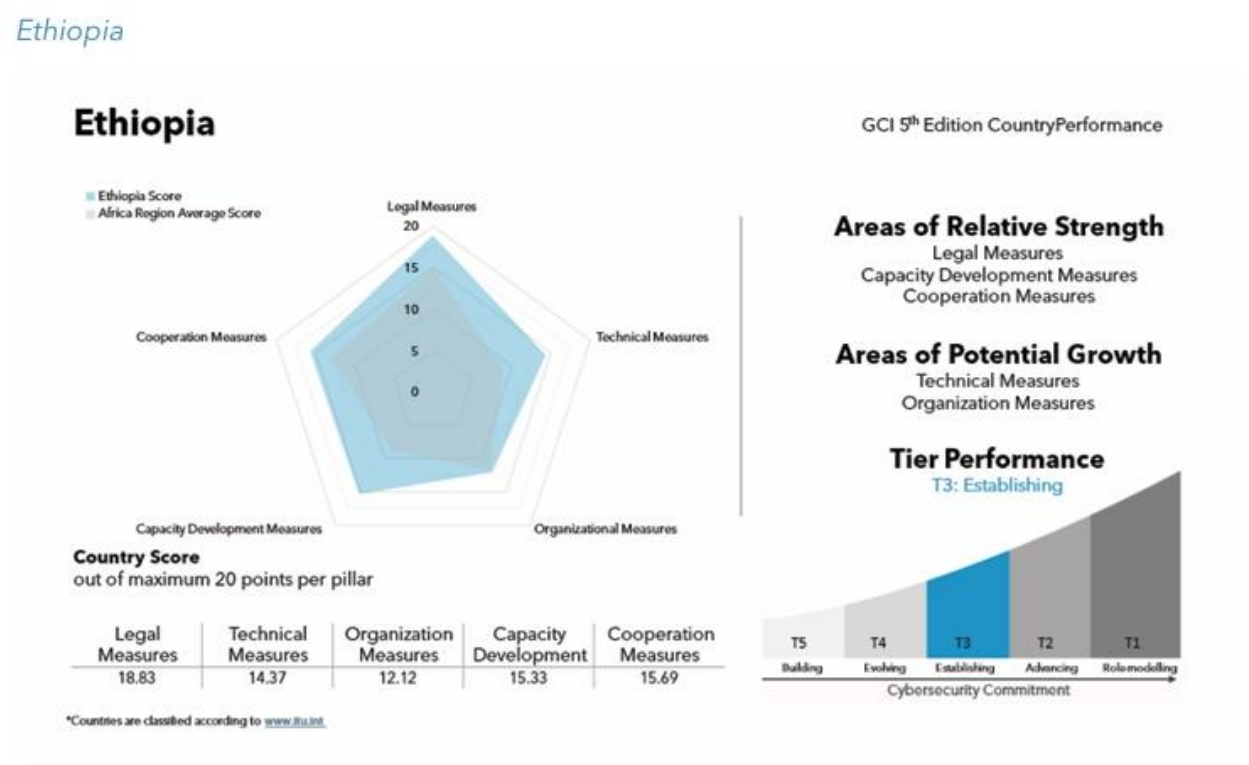

Figure 1:Ethiopian Cybersecurity Commitment (*Source: (ITU, 2024)*)

2.4. Insurance in Ethiopia

The emergence of the modern form of insurance business in Ethiopia and its further development can broadly be categorized into three distinct phases. The first phase (1905-1974) is the emergence and early development of the insurance business in Ethiopia. The second phase (1974-1991) is the nationalization of private insurers and the government's monopoly of the insurance sector. Adopting a market-oriented economic system and

economic liberalization (1991 to date) constitutes the third phase in the historical development of the modern insurance business in Ethiopia.

The first modern insurance was started by a foreign bank named the Bank of Abyssinia (established in 1905), which acted as a foreign insurer to transact fire and marine insurance policies in Ethiopia. The insurance regulatory framework classifies insurance business in Ethiopia into two main classes, namely long-term (life) insurance business and general (non-life) insurance business (Abate & Kaur, 2023).

Insurance regulations in Ethiopia are statutorily enforced by the National Bank of Ethiopia, the primary regulatory body of finance-related businesses. The proclamation that provides permission to deliver an insurance service in Ethiopia does not mention anything regarding cyber insurance. The current active proclamation, which is no 746/2012 (*Proclamation*, 2005), overrides Proclamation no 86/1994, which is the baseline of the insurance business. This regulation was also amended in January 2020 by no 1163/2019, with the aim of amending some articles of the prior proclamation. As mentioned earlier, all three proclamations used as a reference to establish an insurance business in Ethiopia do not state the delivery of cyber insurance in the country. Currently, the insurance industry is regulated by the National Bank of Ethiopia, which has many regulatory directives regarding the insurance business, but nothing has been cited in relation to cyber insurance (Directives, n.d.).

Currently, in Ethiopia, there are 20 insurers operating in the insurance market. Those insurers offer an insurance premium with eight different policies that are clearly stated and one policy with the generic word "others" in it (Members, n.d.)(Profile, n.d.).

2.5. Cyber Insurance

2.5.1. Evolution of Cyber Insurance

Cyber insurance has been around since the late 1970s, evolving from the tech risk and tech errors and omissions (E&O) sector. In the 1980s, the first tech E&O policies that included cybersecurity coverage were introduced, primarily targeting financial institutions and major corporations. The market for standalone cyber insurance began to

grow in response to concerns about Y2K, aiming to address gaps in traditional property and casualty (P&C) coverage (Camillo, 2017).

In the spring of 1997, Steven Haase wrote the first information security liability policy for AIG (Granato & Polacek, 2019). It was also defined as insurance for the damages to "physical" computer equipment in 1970 (Petrović, 2020). Both the growth of ICT and the growing impact of cyber risks towards real-world business increase the demand for insurance-related risk mitigation strategies (Petrović, 2020).

Although the number of insurers offering these products gradually increased, it remained a niche market in its early days. After Y2K, interest in cyber insurance surged due to the dot-com crash and the 9/11 attacks. It became clear that the digital realm often fell outside the coverage provided by conventional insurance policies. Organizations initially worried about the spread of viruses and malware and their associated legal liabilities while also recognizing that cyber incidents could lead to significant business interruption losses not covered by traditional property insurance (Camillo, 2017).

In the beginning, cyber insurance policies mostly focused on companies engaged in information technology, which had taken responsibility for managing networks and systems being used by other companies (Granato & Polacek, 2019). Since then, the market has experienced substantial growth, driven by demand for cyber risk management tools (Article, n.d.).

2.5.2. Cyber insurance market

The current market of cyber insurance has expanded and focused on three forms: *third-party written coverage*, *first-party written coverage*, and *implicit silent cyber coverage*. Since information technology is involved in different business sectors, those varieties of sectors currently adopt cyber insurance policies with different rates across firms and industries (Granato & Polacek, 2019).

There are vital aspects of cyber insurance that make it difficult for insurers to write and price policies. There are a number of factors that are affecting both the demand and supply of cyber insurance (Petrović, 2020). The authors identified seven main reasons as

core points in the case of cyber insurance. In both well-known cyber insurance markets, London and the U.S.A., some risks are identified and categorized clearly as insurable and uninsurable cyber risks (Petrović, 2020).

"Global Risks Report 2024" examines global risks from multiple perspectives, including economic, environmental, geopolitical, societal, and technological domains. The rapid advancement of technology brings both opportunities and risks, including cybersecurity threats, privacy concerns, and the ethical implications of emerging technologies like artificial intelligence (AI) (McLennan, 2024).

Besides identifying cyber risks, cyber insurers may also face challenges in offering cyber insurance to mitigate certain types of cyber risk events (Petrović, 2020). Insurers may prepare their policies in different categories. Among them, cyber incidents that create challenges for organizations are considered by (Aziz et al., 2020). In the industrial era 4.0, many sectors are expected to have cyber insurance. According to (Aziz et al., 2020), cyber insurance coverage has challenges highlighted by different researchers and categorized into three different types. First, before the contractual agreement, i.e., challenges that arise when the insured will use the insurer's services. Second, when a contractual agreement exists between the insurer and the insured, and third, when there is no contractual agreement, the challenges are generally on the cyber insurer.

Different legislations are one of the driving factors for organizations to have cyber insurance for their cyberspace. Based on (Woods & Simpson, 2017), in the U.S.A, UK, and EU, other legislations (which are not part of the cyber insurance) that are developed to protect data may force companies to get cyber insurance. For a wider adoption of cyber insurance, governments may incentivize organizations using different approaches (Woods & Simpson, 2017), among which encouraging organizations to win government contracts by putting cyber insurance as a requirement and buying or getting cyber insurance for government agencies are some of them. Making cyber insurance mandatory in certain business sectors just like other traditional insurance policies is also another adoption technique suggested by (Woods & Simpson, 2017). Cyber insurance may incentivize investment in cyber security, as insurers have been more selective in their risk selection (e.g., only covering those that meet certain cyber security standards). Some

insurers provide services ex-ante, such as pre-breach and virtual CISO services, to improve the security posture of policyholders (IAIS, 2019).

Cyber incidents are the main causes that insurers will be forced to cover the loss if those incidents' data is managed in a way that can be shared among insurers, which is highly recommended in the context of the present cyber insurance insurers (Woods & Simpson, 2017). Information sharing regarding cyber incidents is also credible in preparing sector-based information-sharing practices. Many researchers and scholars have mentioned that a lack of information sharing is a cause of the failure to mitigate cyber threats (Woods & Simpson, 2017).

Different insurers have cyber insurance products, which are different mixtures of alternative features (Kshetri, 2020). These mixed features of cyber insurance policies are considered a problem in the market. The industry is affected by a lack of standard vocabulary and language among sector participants (Kshetri, 2020). Because of its dynamic character, cyber insurance is yet another area that struggles to match the cyber insurance policy with the cyber environment. As mentioned in (Kshetri, 2020), cyber insurance is currently offered as a standalone or add-on service. Cyber insurance has multiple actors who play different roles than traditional insurance. Organizations that have access to personal information in their system might be obliged by regulators to have cyber insurance policies to protect the data collected through the system (Kshetri, 2020). Since cyber risks and cyber-attacks have high dynamicity, organizing a common database to share information within the cyber insurers is highly recommendable (Kshetri, 2020). According to (Farahmand, 2020), the insurance industry follows two approaches to determining the insurance premium: the first is based on the actuarial data and the second is by using normative standards. However, there is no clear evidence which shows how these two standards are applied to cyber insurance premiums.

Organizations that use the same platforms increase the risk of experiencing the same vulnerabilities. Using the same/common platform also has positive externalities, like sharing their cybersecurity information to reduce the damages of cyber-attacks. Those attacks are generated from correlated risks (Vakilinia & Sengupta, 2019),(DHS, 2019). The coalitional cyber insurance framework promoted by (Vakilinia & Sengupta, 2019)

has three major models for ensuring a common platform. The first one is organizations act as both insurers and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, they study the outsourcing of a common platform insurance.

World Economic Forum, in its global cybersecurity outlook report, states that large organizations are more likely to have cyber insurance than small organizations (World Economic Forum Accenture, 2022).

Lack of standardization in cyber insurance is a major challenge outlined in different literature. The other challenges are lack of data, methodological limitations, and information sharing are among them (Kshetri, 2020), (DHS, 2019), (MacColl et al., 2021). As per (DHS, 2019), in theoretical academic literature, as well as in applied research and business publications, the key issues facing the cyber insurance market are divided into two categories. However, the difficulties noted in both categories are very comparable.

2.5.3. Legal and Regulatory frameworks

There was a request for policymakers to reflect on the need for cyber insurance. A ransomware attack disrupted a software company which processed 75% of wool sales in Australia and New Zealand. The requesters argued that regulations that make it mandatory for companies to have cyber insurance could be a way to minimize the disruption (Kshetri, 2020).

In their work, the authors (Lemnitzer & Lemnitzer, 2021) show the importance of cyber insurance for any organization that has cyberspace, and they give more attention to SMEs. The authors argue that the cyber insurance market needs more extensive regulation to overcome market obstacles. Similar to big companies, cyber insurance has an impact on SMEs. Therefore, it should be made compulsory for them to have a time-bound preparation period. The growth of the cyber insurance market is on a fast track in the U.S. and EU. The reason behind this is due to the mandatory data breach notification laws. (Mbatha, 2020) echoed that legislation regarding personal information protection has a positive impact on the growth of the cyber insurance market.

The authors (Lemnitzer & Lemnitzer, 2021) propose six concrete policy to encourage SMEs to be covered by insurers. Promoting the uptake of cybersecurity insurance among SMEs is the first one. The second one is setting a minimum cybersecurity standard for SMEs. On the other hand, regulating the minimum requirements for cybersecurity insurance policies is stated as a third proposal. The fourth one is creating a backstop for systemic cyber risk for insurers and reinsurers. The author discussed encouraging data sharing in the insurance industry and setting up a claims database as a fifth point. The sixth point is announcing an intention to make insurance compulsory for SMEs in the near future.

2.6. Related Works

A number of researchers have studied cyber insurance from different perspectives. Kondwani Makanda et al. (Makanda & Kim, 2017) try to show that in the southern African state of Malawi, there are seven insurance companies, but none of them offer cyber insurance services. Their work focused on measuring the readiness of insurance companies to deliver cyber insurance products in Malawi. The authors (Schwieger & Ladwig, 2022) mentioned the New York Department of Financial Services cyber insurance risk framework in their work. NY DFS developed this framework to be implemented by all insurance companies within the state of New York. The framework has seven steps that need to be fulfilled by both the insurers and the insureds. The framework acknowledges the interdependencies between cyber risk and cyber insurance and the seven steps are also shows this dependency.

The authors (Woods & Simpson, 2017) presented a framework for policy measures and cyber insurance. The author (Wang, 2019) proposes an integrated framework for managing information security investments and cyber insurance. The study explores how organizations can optimize their investments in security and insurance to achieve comprehensive risk management. The framework introduces two components. The first component, investment in security measures, focuses on investing in robust information security measures. This reduces the likelihood of cyber incidents and enhances organizational resilience. The other component is cyber insurance, which complements the security investment with a cyber insurance policy prepared for selected cyber threats

only by providing financial protection against residual risks that cannot be completely mitigated by security measures alone.

The Cyber Risk Assessment and Mitigation (CRAM) framework is introduced by (Mukhopadhyay et al., 2019) to enhance cyber insurance processes using statistical models. The authors integrate two models, logit and probit, to assess and mitigate cyber risk in the context of cyber insurance. The framework focuses primarily on the risk assessment process. The processes involve inputting data into the models to estimate the risk probability. Based on the assessment result, the framework suggests the appropriate mitigation strategies. The author explores the current state of the cyber insurance market in Israel, focusing on the official policies and regulatory framework that influence the market. The cyber insurance market is relatively nascent when compared with more mature markets like the U.S. and Europe. According to the author, the market is growing (Pavel, 2020).

Nur Hidayah Abd Rahman et al. policy (Abd Rahman et al., 2022) stated in their work that a lack of holistic knowledge hinders the development of cyber insurance in Malaysia. The barriers that challenge the growth mentioned by the authors are the cost of premiums and return on investment, which are not convincing for the decision-makers of the potential organizations to buy cyber insurance policies. The other barrier is the lackadaisical attitude toward cybersecurity and cyber risk awareness among many organization employees; the third issue is the lack of evidence and success revealed by the Malaysian regulation, which still lacks legal precedent on cyber security issues. The fourth barrier mentioned by the authors is a lack of standards and policy (Abd Rahman et al., 2022).

2.6.1. Gap Analysis

Many research works have been published on cyber insurance. Their area of focus varies depending on the researcher's intent. In this section, research works used as related work are summarized and presented as follows:

Table 1. Summary of gap analysis

Related works	Focus area	Description (Findings)

Policy measures and cyber insurance: a framework (Woods & Simpson, 2017)	Framework for policy	The researchers offer a framework primarily intended for policy makers to develop and enhance cyber insurance policies and services initially.
Cyber Security Insurance Status in Malawi (Makanda & Kim, 2017)	Readiness assessment	The authors conducted interviews and discussions with insurers to evaluate service availability. If the service was not available, they simultaneously assessed the insurers' readiness to provide it.
Cyber Insurance Concepts for the MIS and Business Curriculum (Schwieger & Ladwig, 2022)	To promote cyber insurance courses on MIS and business curriculum	The researchers want to encourage cyber insurance to be incorporated into the business curriculum to help people acquire trained skills.
Integrated framework for information security investment and cyber insurance (Wang, 2019)	Integrated framework	The researcher used an analytical model to quantify the effect of security investment on cyber threat, vulnerability and impact. It also promotes delivering cyber insurance for itemized cyber threats.
Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance (Mukhopadhyay et al., 2019)	Framework	The authors proposed a framework by using GLM models (i.e. logit and probit).
Cyber Insurance Market in Israel - What is the Official Policy? (Pavel, 2020)	Market analysis	The author analyzes the maturity of the Israeli cyber insurance market and the role of regulatory bodies in the improvement of cyber insurance.
Adoption of Cyber insurance in Malaysia organizations (Abd Rahman et al., 2022)	Market analysis	The authors analyze why the cyber insurance adoption is challenged and lacks progress since there was potential.

In summary, the current body of literature regarding cyber insurance practices is predominantly centered on global market trends, policy development, cyber risk mitigation, cyber insurance policy premium calculation, cyber risk incident response, and other important roles for the cyber insurance policy. The focus is mainly on the positive impact of implementing cyber insurance compared to traditional security investments, using cyber risk assessment and mitigation strategies, and incorporating cyber insurance into academic curricula.

Since cyber insurance is a relatively new concept in Ethiopia, much of the existing literature has been directed toward establishing policy guidelines, understanding the need for regulatory frameworks, and comparing the effectiveness of cyber insurance versus conventional cybersecurity measures. Other discussions in the literature include the integration of cyber risk assessment models in the context of insurance and the necessity of educating future business leaders through business courses on the complexities and importance of cyber insurance. The literature also supports insurers in calculating premiums, which has been identified as a challenge to quantifying cyber risks.

CHAPTER THREE

Research Methodology

3.1. Introduction

This chapter discusses the research methodology, which focuses on the research approach and design, as depicted in Figure 3. The data were collected using structured interviews based on the questions in Appendix B, C and D. The interview questions were designed based on the research questions and the study objective. This was done in an attempt to get a thorough understanding of industry perception to formulate a cyber insurance framework for use in the public and private sectors in Ethiopia. Thematic content analysis was employed to analyze data.

The study will ensure the highest regard for ethical considerations to ensure the transferability and credibility of the research methodology employed. Therefore, this study aims to present a framework by addressing the research question mentioned in this document and to promote the cyber insurance policy for the general public.

3.2. Research Approach

The study employed an inductive research approach. To meet the research objective, interview questions were developed, and interviews were conducted with the identified respondents who have a direct relation to the interview question. The research approach used qualitative methods to collect data. The collected data was analyzed using a thematic analysis approach. As a final output of this research, it delivers a comprehensive framework for use in Ethiopia.

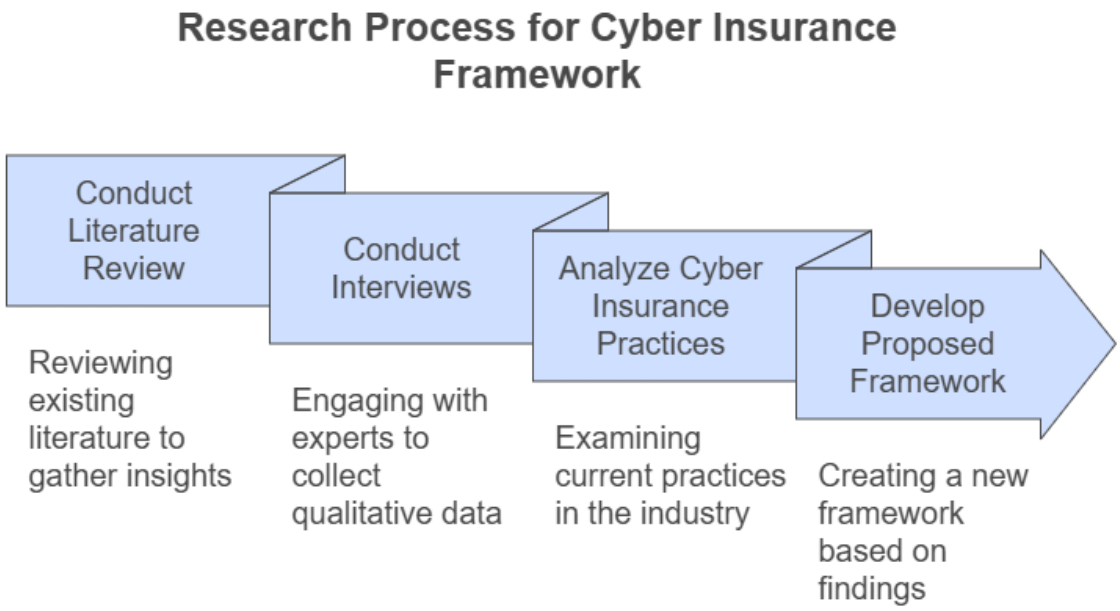

Figure 2.Research Approach

The literature reviewed from different perspectives. In the reviewing process of laws and legislation in the context of cyber insurance, different countries' marketing approaches to cyber insurance, premium calculation, and other related issues are discussed. Based on the existing literature and research questions, interview questions were developed and conducted with relevant stakeholders to implement cyber insurance. Current practices in the cyber insurance industry are also assessed to understand the perception in Ethiopia. Finally, the research proposed a framework that helps to use cyber insurance based on the findings of all the steps in the process. Figure 2 depicts the research process for the cyber insurance framework.

3.3. Research Design

The research design is grounded on the research questions that were framed. An open-ended semi-structured interview was conducted with seven participants who were deemed to possess the necessary experience and understanding of cyber insurance. The research design was comprised of research objectives, which led to three research questions using the interview questions, which are most suitable for a qualitative study to make an inquiry on the cyber insurance concept.

In line with the research objectives and to develop a theory, the study uses an inductive approach. Figure 3 below illustrates the high-level research design presented.

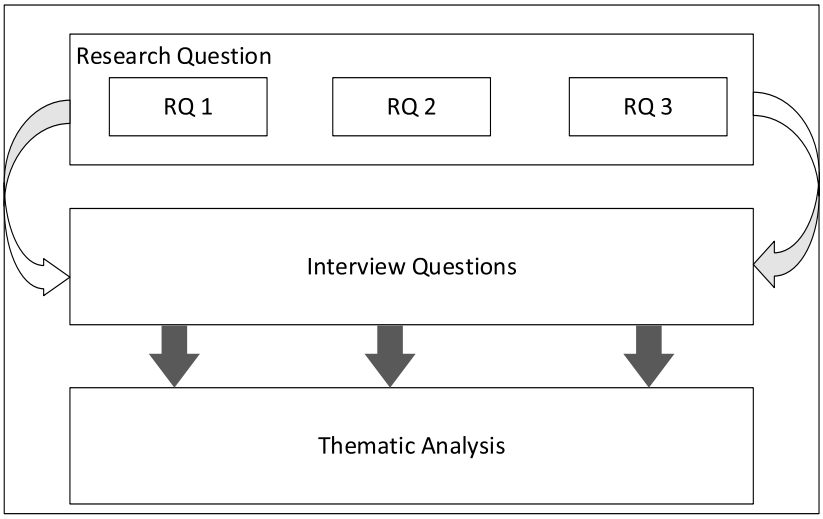

Figure 3. Research Design Summary

The study is conducted by engaging individuals with IT security expertise, insurance service expertise, and regulatory bodies directly related to the insurance industry. Structured interview questions are designed based on the research questions, and thematic analysis will be used to inductively analyze the findings from the semi-structured interview questions. Data analysis is based on thematic content analysis to extract the essence and essentials of participant meanings.

3.4. Data Collection Methods

Structured interview questions were prepared to collect data from the aforementioned parties. The interview was conducted face-to-face with the interviewees. The interview questions were used to enquire about their understanding, interest and expectations related to cyber risk assessment and gave more attention to cyber insurance. The interviewees approached relied on by assuming that they have the capacity to buy a cyber insurance policy, insurance companies that are expected to introduce and deliver this new product for the Ethiopian market, and lastly, the regulatory body that has a mandate to regulate the insurance industry for the sake of the general public.

3.5. Population and Sample

3.5.1. Population

The interview participants were drawn from various disciplines and organizations. The participants' composition was designed carefully to encompass potential cyber insurance policy buyers and the main actors of the industry, which are the insurance companies. Since the regulatory body plays a crucial role in the industry, the study also engaged a participant from the respective body.

3.5.2. Sample and Sampling method

Participants in the interview were selected from a variety of disciplines and organizations for data collection purposes. Five interviewees were from the Information Technology industry with an IT security background, four of whom work in the banking industry, while the fifth is from the energy sector. Additionally, two participants from the insurance sector were interviewed, along with the above-stated representative, who was also interviewed by a regulatory body.

As mentioned earlier, the goal of this research is to promote the importance of cyber insurance policy and to develop a cyber insurance framework, which can be used as a risk mitigation tool for residual cyber risks. Therefore, we performed qualitative research called directed content methodology, or thematic analysis, which identifies themes and concepts that will help extract meanings from the interviewee’s response.

We used the non-probabilistic sampling technique, purposive sampling. Since insurers do not provide a cyber insurance policy, we believes that traversing all the insurance companies registered in the country is unnecessary. Instead of discussing it with all, selecting them based on their year of establishment and size of the company is better. Having this selection, the sample contains insurance companies in a parameter of prominent, private, public, establishment date, and acceptance by the general public.

We identified potential policy buyers based on two key factors: the nature of the business the organization is involved in, and the organization's criticality. If these organizations were to experience a cyber-attack, the consequences would be significant.

The table below shows the respondents' profiles.

Table 2:Summarized list of participants

Description of respondent type	Number to be sampled
Chief Information Officer	1
Information Technology Security Director	3
Cyber Security Director	1
Insurance Underwriting Executive Officer	1
Insurance Sector Regulatory Director	1

3.6.The Research Instrument

The research instrument was prepared based on the qualitative method using structured interview questions designed and constructed in the English language for ease of understanding by the participants. We made a brief describtion on the intent of the questions for the interviewees during the interview session. As mentioned earlier, there were three interview questions, each consisting of 23, 16, and 10 questions for potential policy buyers (holders), policy providers (insurance companies), and regulatory bodies, respectively. Each interview session is recorded to provide a richer pool of data for analysis to be carried out.

3.7.Data Analysis

The data collected using open-ended semi-structured interview questions from research participants purposefully selected from different organizations were analyzed using thematic analysis, and findings were interpreted and discussed accordingly. The recording of the interview was transcribed, and Microsoft Excel was used to extract and present the data to enable the coding. The enabled coding was used in the thematic analysis to synthesize the research question, interview question, and the proposed framework for using cyber insurance in Ethiopia.

3.8.Limitations of the study

Lack of prior experience in a cyber insurance policy from the insurer and insured side limited the study. During the interview study, participants were troubled in understanding or addressing cyber insurance-related questions. Since the insurers were also newbies in cyber insurance policy products, they did not easily understand the new terms, processes,

and technical jargon related to cybersecurity. Thus, their response to the interview question was very limited.

3.9.Demographic Data of the respondents

The study intended to address different participants to incorporate in the interview process. All seven respondents cooperated in reply to the inquiry presented by the researcher. The demographic dispersion is presented in the table below. The table contains participant code, role, sector of the organization, number of total staff and description.

Table 3:Summary of participant's profile

# of Participant	Role	Industry/Sector	# of Staffs	Description
1	Chief Information Officer	Finance Bank #1	More than 5,000	Private business sector
2	IT security Director	Finance Bank #2	6,000 – 7,000	Private business sector
3	IT security Director	Finance Bank #3	More than 12,000	Private business sector
4	IT security Director	Finance Bank #4	Around 2,500	Private business sector
5	Cyber Security Director	Energy	Not mentioned	Public Entity
6	Executive officer, underwriting	Insurance	Not mentioned	Private business sector
7	Insurance sector Director	Public	Not mentioned	Regulatory body

3.10. Ethical Considerations

During the data collection process, confidential data was not gathered or collected. The study does not mention interview respondents' whereabouts, identity and respective organisations. Recordings and transcribed data are kept securely. Interviewees were recorded after getting the respondent's consent.

CHAPTER FOUR

Analysis and Discussion

4.1. Introduction

The preceding chapter on research methodology outlines a structured way to conduct qualitative research to understand the respondents' perceptions during interviews. The interview questions were formulated in an open-ended, semi-structured format. Participants were intentionally chosen based on their direct involvement with insurance services and cybersecurity activities. Chapter four presents and illustrates the findings obtained from these interviews, thoroughly exploring the respondents' views, perspectives, understanding, and interests.

4.2. Thematic Analysis

The study mainly focuses on decision-makers in regulatory bodies, insurance firms to provide contracts (supply side) and potential firms to purchase (demand side) who are likely to purchase cyber insurance policies. Thematic areas were identified based on the replies provided by the aforementioned stakeholders during the interview. These theme areas are classified and summarized as follows.

4.2.1. Ensuring Compliance and Standards

4.2.1.1. Understanding Regulatory compliance

Regulatory compliance is the cornerstone of a responsible business practice. It involves adhering to governing bodies' laws, regulations, and guidelines. In the financial sector, complying with the governance structure is crucial. Currently, in Ethiopia, insurance companies are governed by the National Bank of Ethiopia (NBE). Since most of the interviewees are from the financial sector, they are concerned about understanding regulatory compliance. NBE is the regulatory agency for both the commercial banks and the insurance industry. During the interview, all banks emphasized the importance of complying with all directives and regulations. In fact, in this specific research, the interview mainly focuses on the information security compliance directive SBB/83/2022 issued by NBE. Adhering to regulatory compliance, especially for the financial sector actors, is mandatory because of the huge amount of finance they collect and transact. The impact of non-complying regulatory compliances has a big consequence for the banking industry.

Laws such as the General Data Protection Regulation implemented by the European Union in 2018 made companies increasingly aware of their own potential liability and responsibility and generated greater interest in cyber insurance.

4.2.1.2. Navigating International Standards and Frameworks

According to the interviewees' comments, international standards and frameworks are used to meet their different needs with respect to cybersecurity activities. Almost all of the respondents stated that they employed internationally accepted frameworks such as NIST and ISO 27002. Those frameworks also help them develop their own customized administrative controls like policies, procedures, and guidelines.

4.2.1.3. Accredited Certifiers

There are some banks that hold industry certifications, such as PCI/DSS. The certifier organizations mostly require banks to comply with their standards before they can be certified. These certifiers also have their own standards, which the service requester complies with. According to the interviewees, the standards that certifiers are required to fulfil are customized and mostly used standards or frameworks. Being certified by certifiers is important for every business in the modern era. These certifications are used as a validation to show the organization's commitment to meet the requirements.

4.2.1.4. Mandatory Requirements

Mandatory requirements in some sectors are very crucial. Sectors like healthcare finance have their own special requirements. Those requirements extend beyond legal obligations. Contracts with clients, suppliers, and partners may impose specific compliance conditions. Fulfilling these commitments promotes seamless business relationships. When the interview was conducted, one of the respondents mentioned that due to the lack of cyber insurance services in Ethiopia, their supplier requested that they comply with the supplier's requirement.

4.2.2. Identifying Risks and Ensuring Resilience

4.2.2.1. Understanding risks

Risks cannot be eliminated entirely. This will occur due to the nature of the risks. By their nature, risks will create inherent uncertainty in organizations. There are different sources of risks. They might be sourced in three formats: internal factors, external factors, and technological vulnerabilities. Among these factors, technological vulnerability is the

most sophisticated and becomes more advanced every time. Other than the technological vulnerabilities, the different risks do not have a dynamic behaviour. The interviewees stress that they intend to purchase a cybersecurity insurance policy if they do not handle residual risks in a controlled environment.

4.2.2.2. Risk Assessment

Performing periodic risk assessments is very important. Once the risk assessment is performed, it is easier for top management to make critical decisions. The likelihood and potential impacts are the most important findings that the risk assessment will produce. As per the findings, the organization's management prioritizes and ensures resource allocation. Risk assessment must be visualised based on the severity and likelihood. Risks commonly categorized into three, these are: -

- High Risk – Sever impact, Low likelihood
- Medium Risk – Significant impact, Moderate likelihood
- Low Risk – Limited impact, Higher likelihood

4.2.2.3. Risk Management Frameworks

Frameworks provided structured approaches to managing risks. The financial sector actors used widely accepted risk management frameworks to perform their organizations' risk assessment. The interview respondents showed/declared that they use NIST and ISO frameworks for risk assessment. They also applied INSA’s critical mass framework. According to the respondents, none of them are fully implementing the frameworks developed by the organizations discussed earlier. Banks and other organizations attempt to customize risk frameworks for their purposes instead of fully implementing them.

4.2.2.4. Threats and Threat levels

One of the risk assessment activities is identifying threats. Threats are specific events or conditions that trigger risks. The identified threats should also be assessed to see what levels will be affected if they occur. Identifying threat levels helps organizations plan risk mitigation based on the severity of the risks. Organizations may consider buying a cybersecurity insurance policy as a risk mitigation technique at this stage.

4.2.2.5. Proactive risk mitigation

From the respondent's point of view, they are working proactively to mitigate any possible risks that will cause trouble in their organization.

4.2.3. Cyber Insurance and Coverage Challenges

4.2.3.1. Cyber insurance explanation

Among the four risk mitigation techniques, transferring risk is a recently evolved technique. Technological risks, the so-called cyber risks, are very dynamic. Organizations in place different security measures to mitigate those identified and unidentified risks. After the implementation of all available controls, the residual risks are transferred to a third party. Those third parties are insurance providers who have cyber insurance policies.

4.2.3.2. Components of Cyber Insurance Policies

Cyber insurance policies have some components commonly practised by the insurance industry. Cyber insurance coverage currently has two types: -

- First-party insurance: This covers incidents that happen to the insured organization for financial loss, reputational damage, business interruption, and other relevant damages caused by the incident. Expenses like incident prevention, forensic investigation, etc.… are also covered by this type of insurance policy.
- Third-party insurance covers incidents that create damage to the insured organization's clients.

4.2.3.3. Challenges and Gaps in Cyber Insurance

When the interview was conducted, all the respondents showed their appetite to purchase cyber insurance policies to mitigate the residual risks that will be reflected in their organization. However, there are challenges and gaps that require the attention of every stakeholder. The following challenges are mentioned by the interviewees: -

- Lack of service availability
- Lack of required laws and regulations
- Lack of expertise and guidance
- Lack of trust and clarity were mentioned during the interview process.

4.2.4. Lack of trust, information hiding, lack of clarity

As business entities, insurance providers and their clients must establish and maintain mutual trust. A lack of trust signifies a deficiency in confidence regarding the other party's reliability, integrity, or competence. Organizations, particularly in the wake of cyber incidents, may experience diminished institutional trust. Insurance providers might leverage such incidents for promotional activities, which can be problematic. For clients, especially those in highly competitive sectors like finance, any exploitation of incidents by insurers for marketing purposes can be detrimental. Suppose there is no specific agreement, such as a non-disclosure agreement, between sensitive clients and service providers. In that case, this can lead to a loss of confidence and potentially result in clients withdrawing from their insurance policies.

None of the interviewees were willing to openly admit that they had experienced incidents, breaches, or losses. They only notify regulatory bodies of such events due to compliance obligations. For this study, interviewees responded to questions about incidents by stating that they have not yet encountered any cyber incidents. This reluctance to disclose information may be driven by a desire to avoid revealing vulnerabilities to competitors and the public. However, this practice of withholding information can negatively impact their operations, leading to reduced efficiency, diminished trust, and missed opportunities. The researcher strongly recommends that critical infrastructure organizations, both public and private, collaborate and share data through a dedicated framework or platform to manage better and mitigate risks and incidents.

Another issue identified from the interviews is the lack of clarity surrounding cyber insurance. This issue can be addressed through various techniques. The associated implications can also be mitigated by eliminating the causes of this lack of clarity. Establishing clear communication channels, implementing structured processes, and providing regular updates on relevant information are recommended to prevent ambiguity.

The themes of lack of trust, information hiding, and clarity are interrelated issues that can significantly impact organizational effectiveness and interpersonal relationships. Addressing these issues requires a comprehensive approach that fosters trust, encourages openness, and ensures clear communication and structured processes. By understanding the causes and implications of these themes, organizations can develop strategies to mitigate their effects and enhance overall performance and collaboration.

4.3. Cyber Insurance Framework Synthesization

The table below maps the research questions with the objectives outlined in the specific objectives section of the document. It includes the interview questions directed at relevant stakeholders, encoded themes derived from the respondents' answers, and the components of the proposed framework. This study aims to develop a cyber insurance framework for organizations in Ethiopia. The matrix presented below illustrates the entire research process that has been followed to reach this point.

Each research question is addressed through specific interview questions designed to elicit the respondents' genuine understanding of cyber insurance. All responses are analyzed, categorized, and coded into various themes following the interviews. These encoded themes assist in identifying the suitable framework components to be presented as the outcome of this research paper.

Table 4:Synthesization matrix

Research Questions	Interview Questions	Encoded Themes	Framework Components
1. What are the legal and regulatory frameworks related to cyber insurance in Ethiopia, and their impact on the	i. What type of security sensitive or confidential data does your organization handle? ii. Are you aware of any legal or regulatory requirements related to data	1. Ensuring Compliance and Standards a. Understanding regulatory compliance b. Navigating international standards c. Accredited certifiers	Regulatory Compliance

feasibility of cyber insurance?	protection and cybersecurity that apply to your organization? Are there any regulatory requirements that they should be fulfill to comply? iii. Since most of the insurance policies governed by regulatory bodies, what is the readiness of the regulatory body to promote a new policy for the emerging technology related risks? Future Consideration: iv. What provisions do you think should be in place for future updates or enhancements to the insurance framework?	d. Mandatory requirements	
2. To what extent are organization aware of cyber insurance practices, and how aware are organizations of these practices, and how do they perceive the necessity and	i. Have you ever heard about cybersecurity insurance? If yes, please provide details. ii. Have you considered purchasing cyber insurance before? If yes, please provide details. iii. What specific aspects of your organization's cybersecurity would you like to	1. Cyber insurance and coverage challenges a. Cyber insurance explanation b. Components of cyber insurance policies c. Challenges and gaps in cyber insurance	Define Insurance Coverage Risk Assessment and underwriting Awareness and Education

feasibility of implementing a cyber insurance framework to manage cyber risk? 3. What are the current trends and best practices on cyber insurance?	include in the cyber insurance coverage? (If they experienced it before) What kind of challenges are they face? iv. Are you aware of any specific exclusions or limitations that you would like to include in the cyber insurance policy? v. What is your budgetary allocation for cyber insurance premiums? vi. Does your company requested to offer cyber insurance from your clients? vii. Do you have any initiative/ readiness to provide cyber insurance for the requester? viii. What specific aspects of your organization's cybersecurity would you like to include in the cyber insurance coverage? (If they experienced it before) What kind of challenges are they face? Future consideration: ix. Are there any emerging trends or		

	technologies in the cybersecurity landscape that you believe the insurance policy should address?		
Risk assessment practices	1. Do you currently have any cybersecurity measures in place? If yes, please provide details. 2. Have you ever experienced any cyber incidents or data breaches in the past? If yes, please provide details. 3. If yes, what kind of cost have you ever incurred due to the cyber incident? 4. What are the potential risks and threats your organization faces in terms of cybersecurity? 5. Do you have a dedicated cybersecurity team or personnel responsible for managing and responding to cyber incidents?	1. Identifying risks and ensure resilience a. Understanding Risks b. Risk Assessment c. Risk Management frameworks d. Threats and threat levels e. Proactive risk mitigation	
4. What are the key components of a cyber insurance framework, and how can they be used to effectively manage cyber risks?	1. How your organization handles the incident? 2. Do you have any framework, procedure, or guideline that will be used when incident occur? 3. Do you have a dedicated cybersecurity team or personnel responsible	1. Cyber insurance and coverage challenges a. Cyber insurance explanation b. Components of cyber insurance policies c. Challenges and gaps in cyber insurance 2. Lack of trust, information hiding,	All the proposed framework components

	for managing and responding to cyber incidents? 4. How willing are you to pay higher premiums for broader coverage? 5. Would you require any additional services or support from the cyber insurance provider, such as incident response or risk assessments? 6. What are your expectations from a cybersecurity insurance policy? (e.g., financial coverage, incident response support, legal assistance) 7. Evaluating Insurance Providers: a. What criteria would you consider important when selecting a cybersecurity insurance provider? (e.g., reputation, financial stability, expertise) b. Are there any specific certifications or qualifications you would expect from the insurance provider? 8. Are you aware of any specific exclusions or limitations that you would like to include in the cyber insurance policy?	lack of clarity	

	9. What factors do you think should be considered in determining the insurance premiums? 10. Policy Requirements: a. What types of incidents or losses would you consider as eligible for insurance claims? b. Are there any specific requirements you have regarding the claims process? 11. Policy holder Education and Assistance: a. Do you believe there should be educational resources provided by the insurance provider to help improve cybersecurity practices? b. Should the insurance provider offer assistance in conducting cybersecurity audits or implementing recommended measures?		

4.3.1. Synthesizing RQ 1

The respondents were provided with four questions related to legal and regulatory perspectives to obtain their insights. Among many organizations, the financial industry requires stringent regulation because of the sector's sensitivity. NBE oversees the financial sector and has two massive actors: commercial banks and insurance service providers.

The financial sector should obey rules set by the regulatory body. Among the interview respondents from the banking sector revealed the enquiry ***"****What type of security sensitive or confidential data does your organization handle?****"*** they strongly addressed that they were requested to implement a directive that required putting in place security measures to protect the data that they may collect through their business process. For the above question, the respondents from the banking industry said that they should adhere to the directive, and there is an audit that examines their performance in terms of their compliance with the directive.

The other question raised for the respondents was about regulatory requirements: "*Are you aware of any legal or regulatory requirements related to data protection and cybersecurity that apply to your organization? Are there any regulatory requirements that they should be fulfilled to comply with?*" from the banker's perspective, they are aware of their regulatory body directives, and at the same time, they are also adhering to other international requirements like '*PCI DSS*'. When the interview was conducted, the researcher noticed that there was an inconsistency between them regarding their awareness of regulation. They were considering taking other standards as a regulation. Regulations should be tangled with each other to create a comprehensive security posture.

The same question raised for a participant in the interview from the energy sector responds that there are no regulatory requirements that should be fulfilled to comply.

From the insurance policy providers' perspective, they are obligated to comply with regulatory body regulations. The question "*Since most insurance policies are governed by regulatory bodies, what is the readiness of the regulatory body to promote a new policy for the emerging technology related risks?*" was addressed in the case of promoting a new insurance policy. The service providers should submit their concept notes and other relevant document to get permission to launch a new product. According to the participant from the insurance firm, this regulatory body confirmation is crucial to get the green light and start a new product.

The interview question about provisions regarding future enhancements, "*What provisions do you think should be in place for future updates or enhancements to the*

insurance framework?" was not addressed well. The implication shows a huge gap between understanding emerging technologies and the finance and insurance sector. The insurance industry in this specific area should collaborate with cybersecurity experts, and at the same time, the regulatory body should act accordingly.

The same question was posed to bankers and energy sector participants; however, the limitations observed by the above participant also applied here.

In sum, Ethiopia lacks regulations for cybersecurity insurance.

4.3.2. Synthesizing RQ 2

In his working paper (Geda, n.d.) emphasized that digitalization is generally vendor driven. Alemayehu's point of view was backed by one respondent's response to the question, "*Have you considered purchasing cyber insurance before?*". When the participant described the event, one of their vendors requested a cyber insurance policy to vend his products. The incident allowed them to look after the current cyber insurance practice in Ethiopia. Since there is no provider for this specific insurance product type, they find another way and agree with their vendor to fulfil their need.

The same question was provided for other bankers, insurers, and energy sector participants, but they didn't consider purchasing cyber insurance policies. The reason was stated as a lack of policy providers.

The rapid expansion of digital connectivity is viewed as a key factor driving the need for cyber insurance. According to a report by the ITU (ITU, 2023), mobile broadband subscriptions increased from 1.3 per 100 people to 42 per 100 inhabitants in 2022. Despite the adverse impact of the COVID-19 pandemic, broadband services are becoming more affordable in LDCs. The median cost of a data-only mobile subscription fell from 8.9 per cent of monthly GNI per capita in 2018 to 5.9 per cent in 2022, representing a 34 per cent decrease.

Even though Ethiopia is categorized as an average LDCs group by (ITU, 2023), it is considered a median country because of affordability challenges with data-only mobile broadband plans, which are priced at over 10 per cent of monthly GNI per capita.

However, this status of the country does not mean there is no threat towards digital infrastructures. According to INSA reports (Bedlu, 2023; Behailu, 2023; Endris, 2024; Jemanhe, 2021; Kahsay, 2019; Mohammed, 2022; Reporter, 2020), there are cyber-attacks in different organizations. Those cyber-attack attempts are considered a cyber risk, especially in critical infrastructures.

Taking measures to manage or mitigate residual cyber risk is essential. The interviewees asked if they were aware of cyber insurance in "*Have you ever heard about cybersecurity insurance? If yes, please provide details*", to which five of them replied that they were aware but only to a limited extent. Reading, workshops, training, peer discussions, and vendor requests are all stated as ways to become more informed.

The same question was asked of the insurance company participant. In his response, the awareness was created by their reinsurer, a well-known insurance service in Europe.

Since it has almost no practice in Ethiopia, organizations that participated in the interview process mentioned the inquiry, "*What specific aspects of your organization's cybersecurity would you like to include in the cyber insurance coverage? (If they experienced it before) What kind of challenges are they face?*" the cyber insurance coverage would be better if it included provisions for financial loss, consultation, and risk assessment was among from the listed ones. One responder said that he finds it difficult to speak without the presence of the service.

Lack of explicit or detailed understanding regarding cyber insurance policies, as well as a lack of service availability, have a significant impact on addressing "*Are you aware of any specific exclusions or limitations that you would like to include in the cyber insurance policy?*" answered the question, including the insurer, but they were unable to provide any specific exclusion or limitations to include into the cyber insurance policy.

Even though there are no cyber insurance policy providers currently, the question "*What is your budgetary allocation for cyber insurance premiums?*" was addressed by three bankers who are willing to allocate the necessary budget to buy cyber insurance policies. A participant from the energy replied that top management's limitations about cyber security make it difficult to allocate a budget. On the contrary, one banker addressed this

by questioning the necessity of allocating the budget. The banker argues that he prefers hardening its cyber security posture instead of buying a cyber insurance policy.

The insurer replied to the question, "Does your company request to offer cyber insurance from your clients?" There was a request from banks, but the service provider was not ready. One bank attendee in the interview also replied his bank was requested by a vendor to provide a cyber insurance policy as a guarantee. To fulfil the request, they contacted all insurance service providers, but none of them are currently providing the service.

However, for "*Do you have any initiative/ readiness to provide cyber insurance for the requester?*" an insurer who participated in the interview addressed that they try to customize their reinsurer cyber security insurance policy, but they are not selling it, they believe that the market lost its appetite.

The insurance industry in Ethiopia highly concentrated on traditional policy types. New Insurance policies for new trends or emerging technologies are not open. "*Are there any emerging trends or technologies in the cybersecurity landscape that you believe the insurance policy should address?*" addressed by the insurer participant as if a need had arisen. This shows there is a limitation when introducing a new service.

As a prerequisite to purchasing a cyber insurance policy, cyber risk assessment is very important for insurers and insured parties. In their current cyber security measures organizations," Do you currently have any cybersecurity measures in place? If yes, please provide details," all the participants addressed that they perform risk assessment and in place cybersecurity measurements to protect their data. They try to implement as much as possible.

Regarding the incidents, "*Have you ever experienced any cyber incidents or data breaches in the past? If yes, please provide details*" Since disclosing information has its consequences, all participants were unwilling to address this question, so all of them said they hadn't faced any cyber incident. In "*What kind of cost have you ever incurred due to the cyber incident?*" they replied that they definitely didn't incur any cost regarding the cyber incidents. At the same time, in relation to cyber incidents, all of the participants'

organizations have" *Do you have a dedicated cybersecurity team or personnel responsible for managing and responding to cyber incidents?*" a dedicated cyber security team to manage and respond to cyber incidents. For the question, "*What are the potential risks and threats your organization faces in terms of cybersecurity?*" they responded that all kinds of threats are potential risks for all participants.

4.3.3. Synthesizing RQ 3

The use of organizing a cyber security team in any organization to prevent and handle any cyber incidents. All the participants for" *How did your organization handle the incident?*" responded that based on their governance structure, they established an incident response team. As a matter of fact," Do *you have any framework, procedure, or guideline that will be used when an incident occurs?*" NIST, ISO 27001, PCI DSS, and INSA's Critical Mass framework are used mainly by the organizations. Standards like NIST and ISO 27001 are vast, so instead of implementing as a whole, they commonly try to tailor as per their need and capacity. This experience is helpful for the newly developed cyber insurance framework.

The interview questions were designed to accommodate the possible stakeholder interest in the framework components. The core framework components, which focus on risk assessment and underwriting, are discussed in the previous synthesization sub-topic of this document.

A question raised for participants like, "*Would you require any additional services or support from the cyber insurance provider, such as incident response or risk assessments?*" answered that has a direct impact on component designing. Among the respondents, two required a commitment from the insurer not to disclose any information, which means trustworthiness is a high priority. Other components that focus on premium calculation, coverage definition, and claim processing are related to the interview questions. The participants addressed those questions as challenging to answer because there is a lack of prior experience on the matter, lack of service availability, and lack of awareness is considered as a reason.

4.4. Discussion

In recent years, the growing frequency and sophistication of cyberattacks have significantly impacted both businesses and individuals, highlighting the urgent need for comprehensive risk management strategies. One such strategy, cyber insurance, has emerged as a critical tool in mitigating financial losses resulting from cyber incidents. The study aims to review the legal frameworks that currently exists to regulate insurance services, assesses current insurance practices in Ethiopia including cyber insurance market trends and practices, inurers and insureds perception, feasibility of implementation and mangement thechniques of cyber risks, and propose a newly recommended framework for cyber insurance aiming to establish a more robust, transparent, and adaptive system for managing cyber risk. Next, the discussions are explained in detail.

RQ1: What are the legal and regulatory frameworks related to cyber insurance in Ethiopia, and their impact on the feasibility of cyber insurance?

The study's findings indicate that Ethiopia lacks a regulatory framework for cyber insurance. When the literatures reviewed there was a practice of using regulation to manage cyber insurance policies. In fact, the current world trend of cyber insurance policies is self-initiated, either by the insureds or the insurers. This approach makes it different from other traditional policy types. There are some insurance types generated by different regulatory bodies and delivered to fulfil a regulatory compliance.

The importance of cyber insurance policy is inevitable, and because the product is new to the Ethiopian insurance market, the regulatory body should take proactive steps to manage it well. Insurance companies should promote the service to potential policy buyers and for the general public.

RQ2: To what extent are organizations aware of cyber insurance practices, and how do they perceive the necessity and feasibility of implementing a cyber insurance framework to manage cyber risk?

The awareness level of cyber insurance policy in Ethiopia is very shallow. The interview respondents addressed that there is a huge gap in the awareness perspective. The

mentioned causes are the novelty of the policy throughout the world, lack of adequate promotion regarding the policy, lack of initiative to deliver the service, lack of cyber security expertise to deliver the service are among from them.

Eventhough there was no service provider in the country, there is a potential market to accept this new product and its also reflected when the interview was conducted. There is no doubt from the respondents about the necessity, but when it comes to the feasibility and implementation it requires a collaborative effort from all relevant staeholders. The undeniable fact that all the respondents shared is the cyber insurance product will give a relief by handling residual cyber risks for many organizations.

RQ3: What are the current trends and best practices on cyber insurance?

There is a growing demand for cyber insurance through out the world. Most organizations in Europe and U.S. has an increased risk awareness since cyberattacks raised significantly. Regulatory compliance is the other trend currently observed in the above continents. The cyber insurance coverage models evolved gradually so that insurers are moving from one-size-fits all policies this approach provides a flexibility for the companies to customize the cyber insuance policy. The policies are expanding to include incident respnses services.

The insurance companies currently emphasis on risk mitigation to assess the insurdes security posture assessment to manage risks pre-emptively. The other trend showed in cyber insurance policy is pricing. Due to the increasing frequency and severity of cyberattacks, premiums for cyber insurance are rising. In the mean time insurers are imposing higher deductibles, stricter policy limits, and co-pays for certain incidents to manage growing claims costs.

Cyber threats are borderless, this global reach nature of the risks requires adhering global compliance. Local regulations should be aligned with other continental and regional laws and regulations. In sum, Ethiopian insurers should capacitate themselves and work collaboratively with the cyber security firms and professionals to provide a better service for insurance policy holders.

RQ4: What are the key components of a cyber insurance framework, and how can they be used to effectively manage cyber risks?

To introduce cyber insurance policy to the Ethiopian market and to mange it effectively we proposed a new framework which consists ten different components. The frameworks proposed by different scholars are not provide a holistic solution to utilize and implement it. The proposed framework considers regulatory compliance as a key element. The component suggests that, the regulatory body of Ethiopian insurers should act proactively by providing the required laws and regulations which aligned with other local, regional, and international laws and regulations.

The framework also considers stakeholders participation in the implementation and promotional activities of cyber insurance policies. This engagement from relevant stakeholders also provides a positive out put to used it when the insurance policy coverage is defined. The definition will help to understand the policy inclusion and exclusion when the underwriters prepares the policy.

The proposed frame work contains other important elements like premium calculation, risk mitigation and loss prevention, iincident response and claims process, and other rimportant components which helps both parties (the insured and the insurer) to maximize their benefit from the cyber insurance policy.

CHAPTER FIVE

Proposed Cyber Insurance Framework

5.1.Introduction

The chapter will discuss the proposed solution, which is a cyber insurance framework for use in Ethiopia. The framework contains ten components that have an impact on delivering cyber insurance policy, and each component is discussed well in the component description sub-section of the document. The case study is utilized to evaluate the effectiveness of the proposed cyber insurance framework, and this is also presented as a sub-section in this chapter. Figure 4 illustrates the structure of the framework.

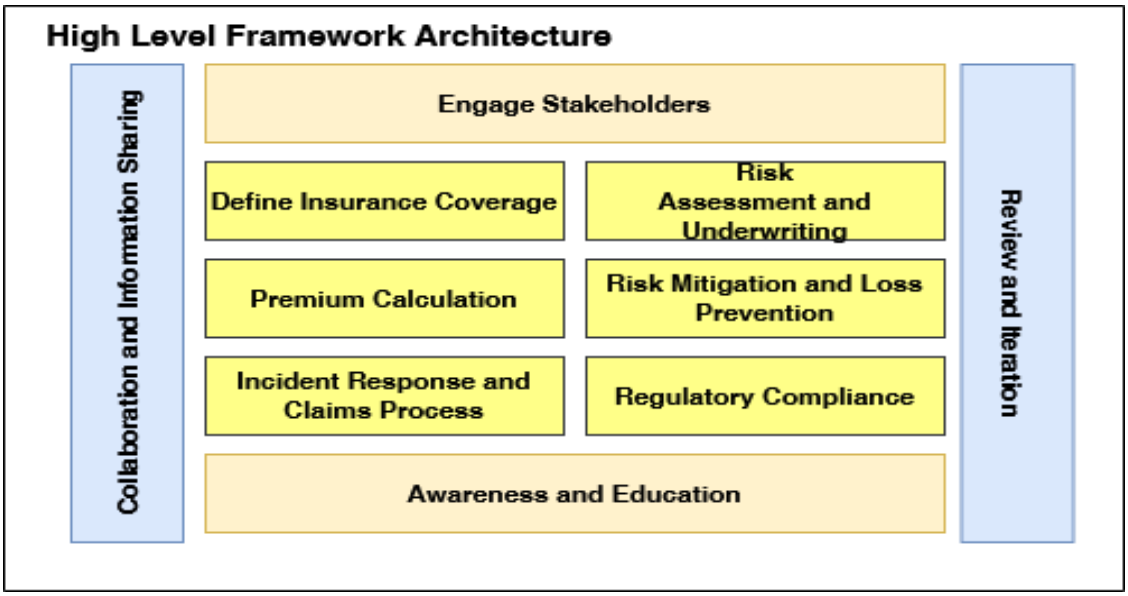

Figure 4. Cyber insurance Framework architecture

5.2.Component Description

1. Engage Stakeholders

Oxford English Dictionary 3 ed., (2004) defines a stakeholder as a compound word that literally meant "the holder of a wager" in its first uses in the 18th century. These days, stakeholders are commonly considered as "persons who have a vested interest in some 'common item'" (Marais & Abi-Zeid, 2021).

Cybersecurity threats are a growing concern for businesses of all sizes. Cyber insurance offers financial protection against these threats, but a robust framework is needed to

ensure its effectiveness. Engaging stakeholders throughout the development of a cyber insurance framework is crucial for its successful implementation and adoption.

This component of the framework outlines a comprehensive stakeholder engagement strategy for creating a cyber insurance framework. The authors (Sachs & Kujala, 2021) mentioned that stakeholder engagement practices have evolved among public, private, and third-sector organizations in recent years, and there is a growing need to further investigate the nuances of stakeholder engagement within organization and management studies. Specifically, various definitions of stakeholder engagement encompass three key ideas. First; stakeholder engagement is viewed as a deliberate action with specific or implicit objectives taken by a firm or organization to address the interests and expectations tied to stakeholder relationships. Second, it involves a range of practices, such as informing, consulting, dialoguing, and making joint decisions with stakeholders. Lastly, stakeholder engagement is expected to influence firm performance and create value for the organization and its stakeholders.

Identify Stakeholders

Marais et al. (Marais & Abi-Zeid, 2021) define stakeholders as those who are characterised by three main characteristics: type of influence, type of participation, and type of visibility.

In this regard, the initial step in developing a cyber insurance framework is identifying the relevant stakeholders. The process involves recognizing the various actors involved at different levels. In this research thesis, the researcher identified and listed the stakeholders who play roles throughout the cyber insurance lifecycle: -

- Regulatory bodies
- Insurance Service providers
- Insurance Service Requesters
- Industry-specific agents
- Third-party actors

Engagement methods

Different stakeholders will have varying needs and preferred communication methods. Here are some effective engagement strategies:

- Workshops
- Conduct surveys
- Interview and
- Advisory committees

Given that the identified stakeholders possess diverse expertise and engage at various levels, it is essential to tailor the engagement methods to each specific stakeholder to manage them effectively. In practice, stakeholders may share one or more engagement methods, but this does not imply that they should be addressed simultaneously.

Communication strategy

Communication is integral to the execution of stakeholder engagement (Smith, 2017). Maintaining clear and consistent communication with stakeholders throughout development builds trust and fosters collaboration. The communication strategy contains a communication plan, message development, regular updates, transparency, and communication channels as a key element.

Engagement of stakeholders in the development process of the cyber insurance framework will provide us with limitless benefits. If all the stakeholders proposed their specific needs and concerns, the framework's effectiveness would increase. The involvement of stakeholders also helps to enhance the adoption of the framework. Stakeholder engagement fosters ongoing collaboration and information sharing between them. Incorporating diverse perspectives leads to a more comprehensive approach to cyber risk management.

By adopting a comprehensive stakeholder engagement strategy, developing a cyber insurance framework can be inclusive and effective and lead to widespread adoption. A well-developed framework will contribute to a more robust cybersecurity ecosystem, protecting businesses from cyber threats and promoting economic stability.

2. Define Insurance Coverage

The lack of a standard cyber insurance policy makes it difficult for customers and brokers to understand and compare the available options. The biggest problem was a lack of education and understanding regarding cyber risks. Most insurance companies worldwide divide the insurance policy into two. *Third-party* coverage and *First party* coverage (Wolf, 2022). In this study of the Ethiopian market, both kinds of policies are recommended.

First-party cyber insurance coverage is intended to assist an organization in responding to data breaches that occur on its own network or systems, including legal bills, investigations, and crisis specialists. Regarding first-party data, an insurer may reimburse costs associated with notifying customers about the data breach, acquiring credit monitoring services for affected customers and undertaking public relations initiatives to repair the company's reputation.

Third-party coverage encompasses issues involving the unlawful disclosure of a third party's information and the infringement of intellectual property rights (IPR). Cyber insurance protects firms in charge of their clients' cybersecurity. Cyber insurance allows them to pay for litigation if their activities or inaction result in a data breach on a client's system. Providers that require third-party cyber insurance include web hosting providers, IT consultants, software and app developers, security consultants, and website designers (Code, n.d.)(Kshetri, 2020).

3. Risk Assessment and Underwriting:

Performing a risk assessment for insurers is very important. The first insurance companies providing cyber insurance policy premiums request to submit a series of tests and assessments performed by the insured company security auditors. Some cyber insurance providers risk assessments for their clients and companies that provide IT services to their clients before agreeing to issue a policy (Wolf, 2022).

The risk assessment process may cover different approaches. When the insured parties respond, questionnaires prepared by the insurer company are the first approach. The

second approach is for insurers to send their own professionals to assess the security posture of that company before issuing the policy.

The authors (Tsohou et al., 2023) mentioned that to address the challenges in risk assessment, they suggest the use of advanced techniques, such as predictive analytics, threat intelligence, and machine learning, to improve the accuracy of risk evaluations and pricing. In their work (Schwieger & Ladwig, 2022), they mentioned that companies that have a quality risk management program with a protective measure will influence the determination of the policy premiums for the insured.

The following diagram depicts participants of this specific component of the proposed framework.

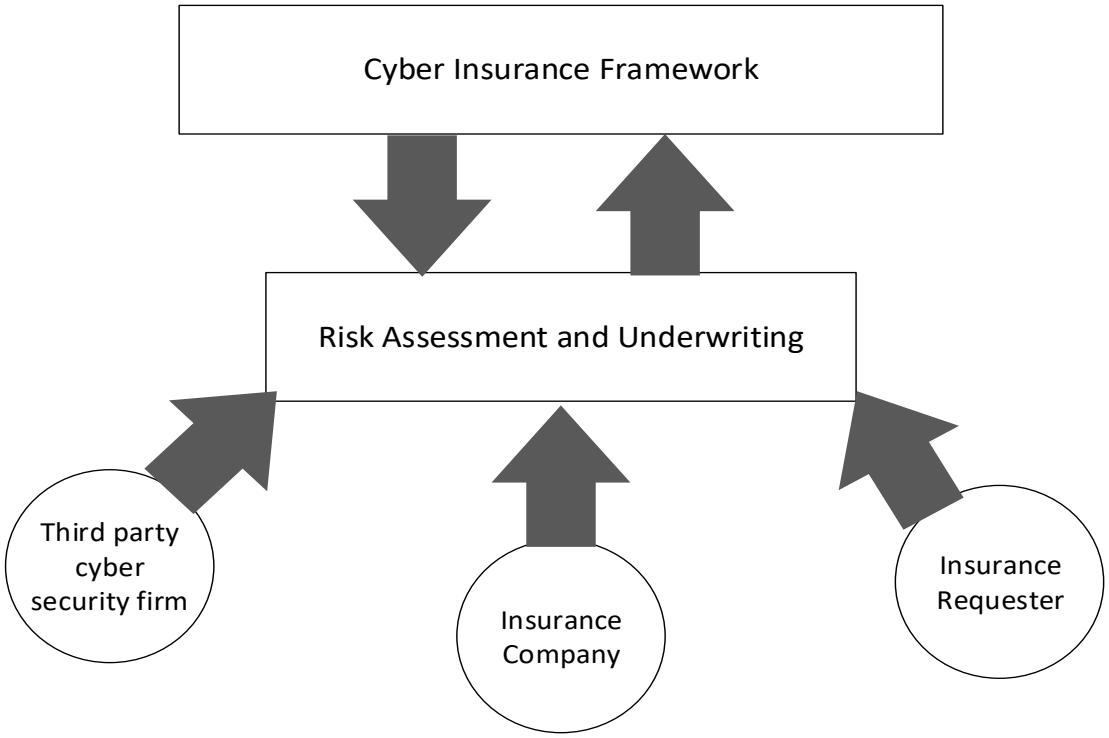

Figure 5. Engaged parties of risk assessment and underwriting component

4. Premium Calculation:

The trend analysis shows that cyber liability coverage prices went downward from 2007 to 2017. This may reflect the effect of growing competition in the cyber insurance market. Carriers are being forced to lure customers from other companies by lowering their prices or even as a new entrants in the market. They use it as a base to cap their price in the market (Wolf, 2022).

There are arguments between regulatory bodies and industry experts on setting premiums. Regulators argue that just like automotive insurance, the insurers should incentivize the insured party to make them more curious and attentive. Different insurers' policies also had very different pricing schemes; this shows that the market lacks standardization to cap a price (Wolf, 2022).

Complex risk assessment is considered a major challenge in cyber insurance, which increases the difficulty in accurately assessing and pricing cyber risks. The dynamic and unpredictable nature of cyber threats makes it challenging for insurers to calculate premiums and coverage limits effectively (Tsohou et al., 2023). Other challenges mentioned by scholars on price determination for cyber risk are lack of historical data, non-stationary claims, association between claims, and strategic moves of threat actors are among them. Besides this rapid growth in exposure without adequate underwriting controls, a growing sophistication of cyber criminals who have been able to exploit vulnerabilities faster than companies can address them, and the far-reaching implication of the cascading effects of cyber risks and the lack of geographic or commercial boundaries also included as a barrier on price determination (Schwieger & Ladwig, 2022)(Zeller & Scherer, 2023).

Historically, insurance pricing has depended on actuarial tables developed from historical data. In contrast, cybersecurity insurance lacks standard scoring systems or actuarial tables for rate setting. Cybersecurity risks are relatively recent, and comprehensive data on security breaches and losses is either scarce or unavailable. This challenge is further compounded by organizations' hesitance to disclose details of security breaches due to

potential impacts on market share and reputation (Xu & Hua, 2019). Cyber insurance service providers may collaborate with cyber security service providers to price cyber risks effectively.

Romanosky et al. studied in their work (Romanosky et al., 2019) how insurance carriers determine a price for cyber risks (formally known as “rate schedules”). The researchers' work mainly focused on the U.S. market only, and they tried to discuss policies provided by insurers residing in the U.S. From their assessment of examined policy providers, four categories were identified. As an umbrella, ‘Flat rate pricing’ and ‘Base rate pricing’ are pricing approaches that use a series of lookup tables and modifiers to compute the premium. The authors also identified other pricing structures when they evaluated policies and coded them as ‘Flat rate with hazard groups’ and ‘Base rate with security questions.’

In a premium setting process, cybersecurity awareness of the insured organization is also a factor in setting the policy content. In the Ethiopian context, setting an appropriate price can be challenging. Both insurance companies and researchers frequently highlight the need for historical incident data. While the insured parties may possess this data, they might be unwilling to share it with other organizations for various reasons. Regulatory bodies overseeing both business and security aspects may need to take on the responsibility of establishing at least an initial pricing framework for insurers and policyholders.

5. Risk Mitigation and Loss Prevention

Risk mitigation has a critical role in cyber insurance. Prevention and preparedness are one of the sub-components of risk mitigation. Cybersecurity assessments, incident response planning and employee training are activities of this sub-component. Performing those activities will help policyholders prevent and prepare for cyber incidents, reducing the overall risk.

Risk mitigation has multiple advantages for both insurers and insureds. Among these advantages provisioned are reducing the frequency and severity of claims. For insurance

service providers, it decreases claims costs; meanwhile, for the insurance service requesters, it will help them enhance their security posture. Cyber insurers may collaborate with cyber security service providers to be in a better position for risk mitigation. Services delivered by the cyber security service providers encompass two parts. The first one, pre-incident, which covers network security, backup of critical systems and data, and patch management, is mentioned. The second part focuses on post-incident services, such as restoration data, forensic services, and legal services (Zeller & Scherer, 2023).

6. Incident Response and Claims Process

The insurance service providers and insurance service requesters may engage equally in incidents. Incidents should be handled using a pre-designed incident response plan. The plan effectively orchestrated how incidents were handled and mitigated risks. In their policies, insurers should clearly show how to handle incidents. After the incidents, the insured may initiate its claim processing. The steps followed by the insured will explicitly be shown in the policy.

The claim process, as the cyber insurance industry experts suggested, begins by collecting data and is used to verify the validity of the claim, understand the nature of the incident, and assess the extent of the damage. Data used includes logs, incident reports, and other relevant data. The claim settlement relied on the data quality and comprehensiveness. This directly affects the speed and accuracy of claim settlement (Jason Nurse et al., 2020).

7. Regulatory Compliance

Regulatory bodies have a crucial role in the implementation of cyber insurance. Different perspectives are expected to be filled by regulatory bodies. Different kinds of regulations, directives, and other required governance techniques should be implemented. Regulatory compliance may not mean gratifying the insurance industry requirements, but it should also cover other country-wide regulations.

Regulatory compliance may cover stakeholders involved in cyber insurance in different modes, the regulatory bodies that manage the business, and the end users, which are companies and individuals. Performing or introducing various kinds of laws increases the sale/purchase of cyber insurance.

As for the other kinds of insurance policies, the cyber insurance policy also requires backing by law to implement the insured party's security measures.

Regulatory compliance covers:

- Customers/clients notification about their PII breaches. This may also be referred to as a data breach law. Which helps protect individuals and companies from theft.
- Provisioning regulatory processes for stakeholders who have a role in the insurance business mainly helps/protects individuals.
- Information sharing on cyber incidents with all relevant regulatory agencies is crucial to the governing process.

Many literature and insurer companies commonly reflect their concern about getting and accessing accumulated data for cyber risks. However, the data collections are not easily accessible or have not even been collected from the beginning. Such limitations should be addressed through different regulatory mechanisms. *GDPR* partially answers such a kind of limitation. In this regard, this thesis will share those points of compliance in the framework.

It is very important when the government takes the initiative to set up policies and regulations. (Pavel, 2020) reviews his paper, the importance of government involvement aimed at promoting cyber resilience, and how these impact the cyber insurance market.

8. **Awareness and Education**:

Cyber insurers should educate companies about cyber security risks and their types. Regular communication with insurance providers and risk management experts ensures organizations stay informed about evolving risks and coverage options.

Scholars recommend promoting initiatives to increase awareness of cyber insurance among businesses, including educational programs and outreach efforts by government and industry organizations (DHS, 2019)(Pavel, 2020).

9. Review and Iteration

Cyber risks are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products, lending to the emergence of cybersecurity insurance as a "Stand alone" line of coverage (Peters, 2017). Cyber insurance policies should be reviewed regularly due to the evolving nature of cyber risks and the rapid growth of cybercrime. As cyber threats change and expand, insurance providers update their policies accordingly. The primary goal of these reviews is to benefit all stakeholders involved in the insurance process. Providers stay current with the latest cyber risks to avoid legal disputes with policyholders and to adjust premium calculations positively.

For policyholders, staying informed about new risks is crucial, as updates from providers offer insight into potential new threats. Additionally, insurance policies related to cyber risks should be reviewed whenever regulatory bodies issue new directives, regulations, or proclamations. Underwriters may miscalculate an organization's cyber risk. As a result, policy holder may be punished financially through a premium based on incomplete or inaccurate data (MacColl et al., 2021). It is advisable for regulatory bodies to request policy reviews as part of compliance for all insurers.

Policy providers can gather feedback from policyholders, as well as other stakeholders such as insurance brokers, consultants, and cybersecurity experts. This feedback is valuable for enhancing the current policies for both providers and holders. Additionally, the feedback process can help to address emerging technology risks that have not yet been identified.

Although, the interviewee from the policy providers describes that reviewing any insurance policy is a common practice. The review process also iterative depends on different situations.

10. Collaboration and Information Sharing:

A problem faced by the cyber realm is the difficulty in gathering data due to the reluctance of organizations to share information regarding past security breaches. This can be attributed in large part to the sizable monetary impact companies suffer due to the loss of trust in their customer base resulting from compromises (Young et al., 2016).

There must be effective strategies to address cyber risks and safeguard the cyber environment from various fraudulent activities. While government and private institutions play crucial roles, individuals also need to actively protect themselves from inappropriate cyber activities. Prevention and protection are ongoing efforts that require sustained collaboration among multiple stakeholders and a reliable information-sharing platform.

This platform facilitates the exchange of information about cyber incidents, identified threats, and emerging risks. To ensure protection against further cyberattacks, the data-sharing process should be anonymized. The platform may include key participants in the cyber environment, such as cyber insurance policy providers, regulatory bodies, cybersecurity firms, and consultants. Through this collaborative approach, these stakeholders can enhance threat intelligence and improve risk mitigation.

5.3. Case Study

In this case study, policyholders and insurers have taken steps stated below which are relied on the proposed framework. The case study demonstrates how the cyber insurance policy will be provided to a potential buyer who wants to mitigate its residual cyber risks.

Introduction

An organization named XYZ PLC perform a holistic/comprehensive risk assessment. Based on their strategic document and risk mitigation plan, the team responsible for this task will provide a solution for the identified risks.

As part of the risk assessment team member and the XYZ PLC chief information officer (CIO), cascade technological risks which are expected to be solved by the IT security team. Based on their capacity and the company's potential, the team lists and categorizes risks that are identified by the risk assessment team. According to their risk appetite, when they categorize risks, some are accepted and mitigated by the security controls that have been deployed.

Some of the categorized risks will be avoided by strengthening their cyber security posture. After doing this, the team discussed thoroughly how they would address the residual cyber risks not addressed by the known risk mitigation techniques and finally decided to transfer the residual risks to a third party, which means buying an insurance policy from an insurance company, who provides a cyber insurance product.

Finally, the team proposes their solution for the top management to manage the residual risks by acquiring cyber insurance policy. The management then takes appropriate action to implement the suggestion.

Step one – Request Form

The board of management discussed the proposal carefully and sent a positive signal to proceed as per the request. XYZ PLC wrote an expression of interest letter to buy a cyber insurance policy from Trust S.C., an insurance company legally registered and operated in the country. The insurer then requested that XYZ PLC fill out the appropriate application prepared by the company.

Step two – Application Review

The insurer (policy provider) reviews and analyzes the application and prepares a meeting with the insurance requester. The meeting focused on briefing both parties regarding the requested policy. The cyber insurance policy provider shows the cases, policy coverage, and steps the potential cyber insurance policyholder should take. After the briefing, the insurer delivers a document which has an exhaustive list of questions that are expected to be addressed by the insured.

Step three – Document and Physical Evaluation

Accompanying the above-mentioned questionnaire, the insurer also requested all the necessary documents from the insured:

- Regulatory compliance
- International standards
- Risk management related documents
- Industry specific standards

The insurer thoroughly checked the documents delivered by the holder. The insured should be able to adequately describe and maintain its administrative, technical, and physical controls. After all the documentation processes are finalized, the insurer company decides to make a site visit to check some requirements, which may verified by the eye-witnessing approach. Physical security, data center facilities, and other relevant issues will be addressed in this step.

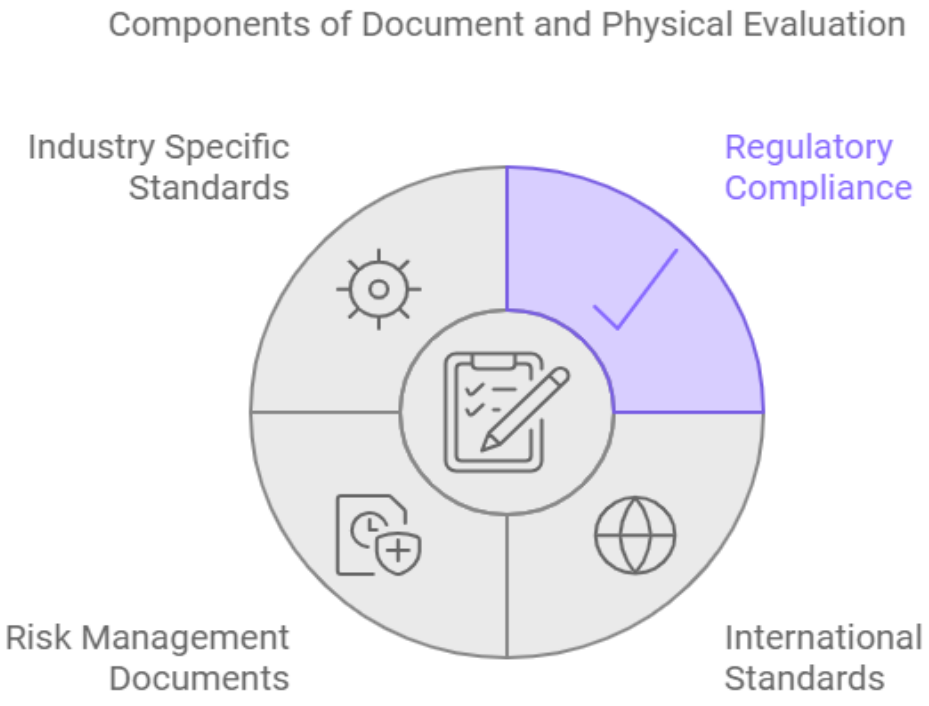

Figure 6. Documents and Physical evaluation

Step four – Third-party Evaluation

The insurance company will decide whether to conduct a risk assessment depending on the results collected from the preceding processes. Since performing risk assessment in terms of cybersecurity requires expertise, the policy provider decides to hire a company who has a reputation for this service. The hired company performed a comprehensive risk assessment by using selected risk assessment frameworks and tools and delivered its final report to the insurance company.

Step five – policy providing

The insurance company compiles all results from the pre-underwriting processes, which include the insurance service request form completed by the policy buyer, the submitted documents and returned questionnaires, and the risk assessment report conducted by a third-party cybersecurity firm. Based on this aggregated information, the insurer agrees to issue the requested insurance policy to the insured.

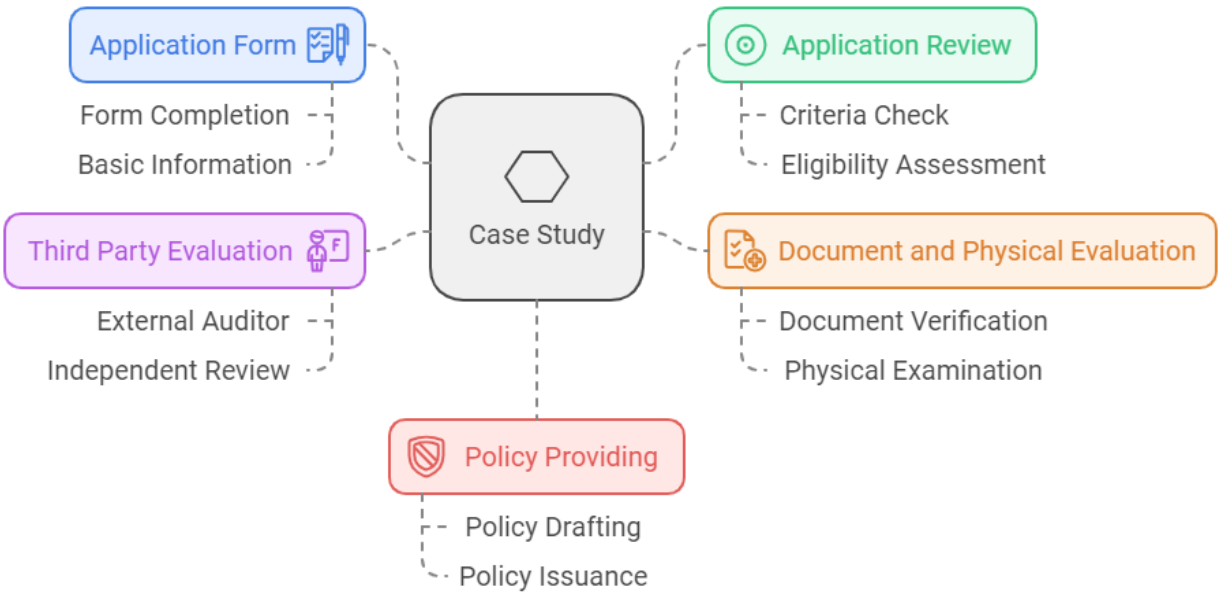

Figure 7. Summary of Case Study

CHAPTER SIX

Summary and Future work

This section provides a comprehensive summary of the key findings and insights derived from the analysis conducted in the preceding sections. The objective is to present a clear and concise overview of the key points, focusing on the most important aspects and their implications. Based on the analysis, this section will also offer recommendations aimed at the implementation of cyber insurance framework, with the goal of providing actionable guidance for future work. By synthesizing the information, the summary aims to give a clear understanding of the core takeaways, while the recommendations provide a pathway for cyber insurance framework.

6.1. Summary

This study proposed a cyber insurance framework for Ethiopia. The proposed framework has considered the current cyber insurance practices in Ethiopia organizations (both the insurer and insured), current market trends, the future plan towards digitalization from the government perspective, as well as the insurance regulatory frameworks. The framework presented to the insurance industry to provide a cyber insurance policy in Ethiopia.

To develop the framework, we studied different stakeholders who have stakes in the industry. Furthermore, different literatures reviewed to understand the current trend of cyber insurance, and related works also searched to findout the limitations. The framework has ten components clearly showed that how the framework functioned. The components intertwined each other, even though the components function solely, but they will provide huge impact when we compiled them collectively. The components clearly presented and displayed for the insurance industry how to deliver the cyber insurance policy for policy holders.

The framework validation process presented in a case study format. In the case study components of the framework which are considered as a core traversed and stated when case study showed. The case study helps to show the credibility and applicability of the framework. The proposed framework should always be enhanced through time to time to adapt the new risks, emerging technologies and regulatory requirements.

6.2. Recommendations and Future work

Cyber insurance is a new trend and a new product for the insurance industry. Even though this insurance type is in its infancy stage, Ethiopian insurance companies should promote the product for potential insurance policy buyers. At the same time organizations who has currently digitalized their business and critical infrastructures should buy a cyber insurance policy to mitigate residual cyber risks. Regulatory body of the insurance industry should also provide the required regulations to encourage both parties to participate in the cyber insurance policy.

As a future work, the framework can be enhanced to accommodate emerging technologies like Artificial Intellegence, IoT, and even 5G technology. The framework also be adapted to be applied in all critical infrastructures too.

REFERENCES

Abate, M. T., & Kaur, R. (2023). Insurance Sector in Ethiopia: Evolution and Current State. *Eur. Chem. Bull*, *12*(5). https://doi.org/10.31838/ecb/2023.12.si5.077

Abd Rahman, N. H., Raju, R., Ariffin, S., Abdul Hamid, N. H. A., & Ahmad, A. (2022). Adoption of Cyber Insurance in Malaysian Organisations. *International Journal of Innovative Computing*, *12*(2), 45–51. https://doi.org/10.11113/ijic.v12n2.380

Adane, K. (2022). The Current Status of Cyber Security in Ethiopia. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3545189

Article, E. R. (n.d.). *No Title*. Retrieved July 4, 2023, from https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Aschenek Zeleke, T. (2019). The Quandary of Cyber Governance in Ethiopia. *Journal of Public Policy and Administration*, *3*(1), 1. https://doi.org/10.11648/j.jppa.20190301.11

Aziz, B., Suhardi, & Kurnia. (2020). A systematic literature review of cyber insurance challenges. *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, 357–363. https://doi.org/10.1109/ICITSI50517.2020.9264966

Bedlu, B. (2023, October 28). Risk-based approach, capacity building set Ethiopia cyber resilient:INSA. *The Ethiopian Herald*. https://press.et/herald/?p=83990

Behailu, M. (2023, October 31). INSA Underscores intensifying efforts against cyber attacks. *The Ethiopian Herald*. https://press.et/herald/?p=84117

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63. https://doi.org/10.1080/23738871.2017.1296878

Code, L. (n.d.). *The Study on Willingness to Pay for Cyber Insurance in Thailand 태국의 사이버보험 지불의사에 관한 연구*.

DHS. (2019). *Assessment of the cyber insurance market*.

Directives, I. business. (n.d.). *No Title*. Retrieved May 30, 2023, from https://nbe.gov.et

Ebert, C., & Duarte, C. H. C. (2018). Digital Transformation. *IEEE Software*, *35*(4), 16–21. https://doi.org/10.1109/MS.2018.2801537

Endris, Y. (2024, August 11). No Title. *News Paper*. https://press.et/herald/?p=100363

Farahmand, F. (2020). Quantitative Issues in Cyberinsurance: Lessons from Behavioral Economics, Counterfactuals, and Causal Inference. *IEEE Security and Privacy*, *18*(2), 8–15. https://doi.org/10.1109/MSEC.2019.2930054

Geda, A. (n.d.). *Working Paper DT-00 1*.

Proclamation, (2005) (testimony of Government).

Granato, A., & Polacek, A. (2019). The growth and challenges of cyber insurance. *Chicago Fed Letter*, *426*. https://doi.org/10.21033/cfl-2019-426

IAIS. (2019). *Global Insurance Market Report [GIMAR] 2018*. *7*. www.iaisweb.org

ITU. (2023). *Measuring digital development Facts and Figures: Focus on Least Developed Countries*. *March*, 1–29. www.itu.int

ITU. (2024). *ITU Publications International Telecommunication Union Global Cybersecurity Index 2024 5 th Edition Global Cybersecurity Index 2024 5th Edition Acknowledgements*.

Jason Nurse, R. C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020). The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*, 1–8. https://doi.org/10.1109/CyberSA49311.2020.9139703

Jemanhe, Y. (2021). Strengthening cybersecurity for national security. *The Ethiopian Herald*. https://press.et/herald/?p=45045

Kahsay, D. (2019, November 2). Agency foils 80 percent of attempted cyber attacks last year. *The Ethiopian Herald*. https://press.et/herald/?p=15020

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy*, *44*(8). https://doi.org/10.1016/j.telpol.2020.102007

Lemnitzer, J. M., & Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory compulsory. *Journal of Cyber Policy*, *0*(0), 1–19. https://doi.org/10.1080/23738871.2021.1880609

MacColl, J., Nurse, J. R. C., & Sullivan, J. (2021). Cyber insurance and the cyber security challenge. *RUSI Occasional Paper*.

Makanda, K., & Kim, H. (2017). Cyber Security Insurance Status in Malawi. *International Journal of Applied Engineering Research*, *12*(17), 6983–6987. https://www.ripublication.com/ijaer17/ijaerv12n17_90.pdf

Marais, A., & Abi-Zeid, I. (2021). *A Method to Identify, Characterize and Engage Relevant Stakeholders in Decision Processes*. https://doi.org/10.13140/RG.2.2.23890.89287

Mbatha, N. S. (2020). *Factors influencing cyber insurance adoption in South Africa industry Nkosinathi Sphiwe Mbatha*. *2020*.

McLennan, M. (2024). Global Risk Report 2024. In *Word economic forum*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Members. (n.d.). *No Title*. Retrieved May 30, 2023, from https://www.associationofethiopianinsurers.com

Mohammed, A. (2022, July 31). INSA foils cyber-attacks on mega projects. *The Ethiopian Herald*. https://press.et/herald/?p=58058

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, *21*(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

Pavel, T. (2020). Cyber Insurance Market in Israel - What is the Official Policy? *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*. https://doi.org/10.1109/CyberSA49311.2020.9139722

Peters, G. (2017). *WORKING PAPER 18-01*. *January*. https://doi.org/10.2139/ssrn.3065635

Petrović, S. (2020). Cyber insurance. *Pravo i Privreda*, *58*(1), 206–217. https://doi.org/10.5937/pip2001206x

Profile, I. (n.d.). *No Title*. Retrieved May 30, 2023, from https://www.associationofethiopianinsurers.com

Reporter, S. (2020, June 24). INSA halts cyber-attacks orchestrated by Egypt. *The Ethiopian Herald*. https://press.et/herald/?p=24517

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz002

Sachs, S., & Kujala, J. (2021). *Stakeholder Engagement in Management Studies: Current and Future Debate*.

Schwieger, D., & Ladwig, C. (2022). *Cyber Insurance Concepts for the MIS and Business Curriculum*. *20*(December), 54–66.

Smith, P. A. (2017). Stakeholder Engagement Framework. *Information & Security: An International Journal*, *38*, 35–45. https://doi.org/10.11610/isij.3802

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, *22*(3), 737–748. https://doi.org/10.1007/s10207-023-00660-8

Vakilinia, I., & Sengupta, S. (2019). A Coalitional Cyber-Insurance Framework for a Common Platform. *IEEE Transactions on Information Forensics and Security*, *14*(6), 1526–1538. https://doi.org/10.1109/TIFS.2018.2881694

Wang, S. S. (2019). Paci fi c-Basin Finance Journal Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*(June), 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Wolf, J. (2022). *Cyberinsurance policy : rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks*. The MIT Press,.

Woods, D., & Simpson, A. (2017). *Edinburgh Research Explorer Policy measures and cyber insurance : a framework Policy measures and cyber insurance : a framework*. *2*(2), 209–226. https://doi.org/10.1080/23738871.2017.1360927

World Economic Forum Accenture. (2022). Global cybersecurity outlook 2022. *Insight Report, Cybersecurity Outlook 2022*, 35. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

Xu, M., & Hua, L. (2019). Cybersecurity Insurance : Modeling and Pricing Cybersecurity Insurance : Modeling and Pricing. *North American Actuarial Journal*, *23*(2), 220–249. https://doi.org/10.1080/10920277.2019.1566076

Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, *14*, 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001

Zeller, G., & Scherer, M. (2023). Risk mitigation services in cyber insurance: optimal contract design and price structure. *Geneva Papers on Risk and Insurance: Issues and Practice*,

48(2), 502–547. https://doi.org/10.1057/s41288-023-00289-7

APPENDICES

Appendix - A Baseline Assessment

1. Why your organization needs/requires to purchase cybersecurity insurance?

   Ans

   - There is no any enforcement to buy cybersecurity insurance from the regulatory body.
   - The shareholders of the company have interest on buying cybersecurity insurance, so that when they establish the business here in Ethiopia, they also require to purchase insurance for their business. This is a second factor of purchasing cybersecurity insurance policy.
   - The business domain they engaged has high risk for cyberattack. So, as a mitigation technique for those high risks they have to be purchase cybersecurity insurance for their business.

2. Have you conducted a comprehensive cybersecurity risk assessment?

   Ans

   - They made their own risk assessment before they acquire the insurance policy.

3. Have you tried to reach any local insurance company to purchase cybersecurity policy?

   Ans

   - Based on the response, Ethiopian Insurance regulation does not allow purchasing any insurance abroad. In a matter of fact, there is no any insurance company can able to deliver cybersecurity insurance policy locally.
   - Since the regulation is not allowed purchasing from foreign companies, the purchasing process must be pass through the local insurance companies. So that, the responsive party of this questionnaire purchase this insurance policy through its local insurance policy provider.

4. Did you explore different insurance providers and their cybersecurity insurance offerings?

   Ans

   - The group (a collection of shareholders who are gathered to form a company to run the business) has a dedicated insurance consultant. Among from its different tasks, the consultant should perform exploring

appropriate insurance providers with offerings performed. The consultant selects the best fit for the group based on their own criterion.

5. What kind of parameters were being used to select your current cybersecurity insurance provider?

   Ans

   - The selection process and the entire process was performed by the insurance consultant

6. Does a buyer of cybersecurity insurance need assistance from knowledgeable professionals including insurance brokers and agents?

   Ans

   - Yes, because we still have lack of capacity or deficit on this field. To promote this new policy for the industry getting knowledgeable professionals are very important

7. Following the selection process of your insurance provider, what were the steps/phases you passed through before acquiring the policy?

   Ans

   - The insurance company requests to fill the proposal they required from the insurers. The proposal submitted to the insurance company. The insurers also present their current security posture before getting the insurance policy.

8. How often the insurance company review your cybersecurity practices?

   Ans

   - Based on their agreement cybersecurity practices of the insured party reviewed annually.

9. How the organization select the policy type, if the insurer provides different kinds of policies? (Exclusion, limitations, etc.…)

   Ans

   - Even though the group consultant handles the entire process, they are aware of that the insurance policy that they have full coverage which is a comprehensive type of policy.

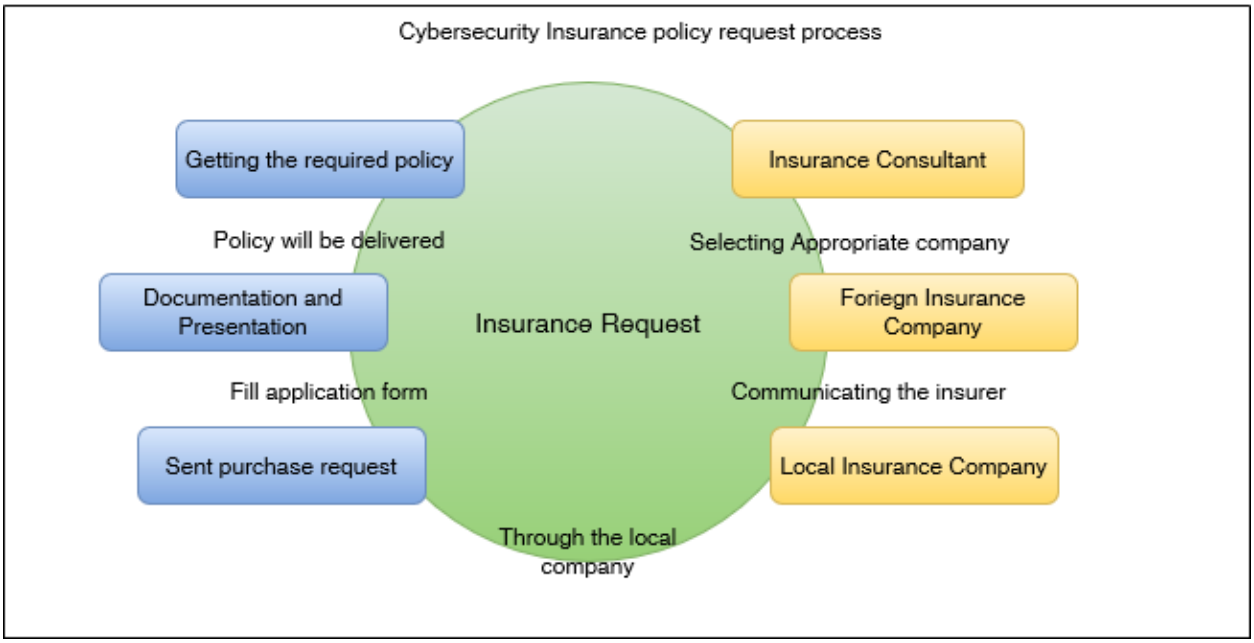

Figure 8. Steps performed by cyber insurance policy holder

Appendix - B Interview Question 1

Interview Question for Insureds

1. Demographic and Company related general information.

   a. Name of the organization:
   b. Industry sector:
   c. Size of the organization (number of employees):
2. What is the nature of your business or organization?
3. What type of security sensitive or confidential data does your organization handle?
4. Do you currently have any cybersecurity measures in place? If yes, please provide details.
5. Have you ever experienced any cyber incidents or data breaches in the past? If yes, please provide details.
6. If yes, what kind of cost have you ever incurred due to the cyber incident?
7. How your organization handles the incident?
8. Do you have any framework, procedure, or guideline that will be used when incident occur?
9. What are the potential risks and threats your organization faces in terms of cybersecurity?
   How would you rate the level of cyber risk exposure for your organization?

Table 5:Rating loss severity

Depends on the Impact that has been occurred in the organization the following points will help to rate the level of cyber risk	High	Medium	Low
• Financial loss			
• Business Interruption			
• Reputational Damage			
• Time taken to resume business			

   a. Have you conducted a comprehensive cybersecurity risk assessment? If yes, briefly describe the findings.
   b. Do you have any frameworks, Procedures, guideline etc. to perform cyber security risk assessment? If yes, please provide details
10. Are you aware of any legal or regulatory requirements related to data protection and cybersecurity that apply to your organization? Are there any regulatory requirements that they should be fulfill to comply?
11. Do you have a dedicated cybersecurity team or personnel responsible for managing and responding to cyber incidents?
12. Have you ever heard about cybersecurity insurance? If yes, please provide details.
13. Have you considered purchasing cyber insurance before? If yes, please provide details.

14. What specific aspects of your organization's cybersecurity would you like to include in the cyber insurance coverage? (If they experienced it before) What kind of challenges are they face?
15. Are you aware of any specific exclusions or limitations that you would like to include in the cyber insurance policy?
16. What is your budgetary allocation for cyber insurance premiums?
17. How willing are you to pay higher premiums for broader coverage?
18. Are you open to implementing recommended cybersecurity measures to potentially reduce premiums or deductibles?
19. Would you require any additional services or support from the cyber insurance provider, such as incident response or risk assessments?
20. Are there any unique requirements or considerations specific to your industry that should be accounted for in the development of the cyber insurance framework?
21. Policy Requirements:
    a. What are your expectations from a cybersecurity insurance policy? (e.g., financial coverage, incident response support, legal assistance)
22. Evaluating Insurance Providers:

    a. What criteria would you consider important when selecting a cybersecurity insurance provider? (e.g., reputation, financial stability, expertise)

    b. Are there any specific certifications or qualifications you would expect from the insurance provider?

23. Future Considerations:

    a. Are there any emerging trends or technologies in the cybersecurity landscape that you believe the insurance policy should address?

    b. What provisions do you think should be in place for future updates or enhancements to the insurance framework?

Appendix - C Interview Question 2

Interview Questions for Insurers

1. Demographic and Company related general information.

    a. Name of the organization:
    b. Industry sector:
    c. Size of the organization (number of employees):

Traditional/Existing Policy approach

2. How the traditional insurance policy works?
3. Does each insurance companies have a mandate to produce/create new policy?
4. What is the development stage/phase of other insurance products?
5. What is the legal precedence on policy offering for a new policy?
6. Do you have a practice of processing for gathering, analyzing and sharing information in the traditional policy coverage?
7. Since most of the insurance policies governed by regulatory bodies, what is the readiness of the regulatory body to promote a new policy for the emerging technology related risks?

Cyber Insurance readiness

8. Have you ever heard about cybersecurity insurance? If yes, please provide details.
9. Does your company requested to offer cyber insurance from your clients?
10. Do you have any initiative/ readiness to provide cyber insurance for the requester?
11. What specific aspects of your organization's cybersecurity would you like to include in the cyber insurance coverage? (If they experienced it before) What kind of challenges are they face?
12. Are you aware of any specific exclusions or limitations that you would like to include in the cyber insurance policy?
13. What factors do you think should be considered in determining the insurance premiums?
14. Policy Requirements:
    a. What types of incidents or losses would you consider as eligible for insurance claims?
    b. Are there any specific requirements you have regarding the claims process?

15.Policyholder Education and Assistance:

    a. Do you believe there should be educational resources provided by the insurance provider to help improve cybersecurity practices?

    b. Should the insurance provider offer assistance in conducting cybersecurity audits or implementing recommended measures?

    16. Future Considerations:

a. Are there any emerging trends or technologies in the cybersecurity landscape that you believe the insurance policy should address?

b. What provisions do you think should be in place for future updates or enhancements to the insurance framework?

Appendix – D Interview Question 3

1. What are the baseline requirements to introduce a new insurance product to the market?
2. How does the regulatory body ensure that insurance companies comply with these regulations?
3. What is the process for approving a new insurance product?
4. How do you evaluate the risk management practices of insurers?
5. What challenges does the insurance industry faces currently? How the regulatory body respond to those challenges?
6. Does the regulatory body set policy and coverage for insurers? If so, what are the steps?
7. Are the insurers expected to adhere industry standards to offer an insurance policy?
8. What role does the regulatory body play in fostering collaboration between insurers, cybersecurity experts, and other stake holders?
9. Does the regulatory body engage in price setting?
10. Is there any plan to introduce insurance products based on the new emerging technologies?