Challenges and Readiness for Cybersecurity Threats at Selected Private and Governmental Banks

Betelhem Kidane Lema
HiLCoE School of Computer Science and Technology, Addis Ababa, Ethiopia
bent.nebo@gmail.com,

Tibebe Beshah
HiLCoE School of Computer Science and Technology, Addis Ababa, Ethiopia
tibebe.beshah@gmail.com

Abstract

The risk level from cybersecurity threats faced by banks has surged in recent years due to the global increase in cyberattacks, with banks being prime targets. Sensitive data and organizational security are at significant risk due to these escalating threats. This situation is exacerbated by the absence of a standardized cybersecurity framework to safeguard online financial data transfers between banks and their clients. To address these challenges, a new cybersecurity framework has been developed, serving as a guide for financial institutions to protect their data effectively.

To meet the research objectives, a mixed-method approach, incorporating both quantitative and qualitative methods, was employed. The survey questionnaire and interview outline were created by partially adapting existing and developing new ones as needed. Cybersecurity professionals from the Commercial works Bank of Ethiopia, Development Bank of Ethiopia, Nib International Bank, and Tsedey Bank participated in this study. The quantitative component involved 50 respondents from both private and government banks, representing a variety of job titles, responsibilities, and work histories. For the qualitative study, direct interviews were conducted with four bank cybersecurity directors. Alternatively, the researcher could use the census approach, also known as the complete enumeration survey method. Quantitative data were analyzed using the SPSS software program and relevant descriptive statistical procedures, while open coding techniques were used for the qualitative data analysis.

The study results indicated that social engineering attacks (59.1% in private banks and 71.5% in government banks), phishing attacks (45.4% in private banks and 46.4% in government banks), and DDoS attacks (32.1% in private banks and 22.7% in government banks) are the most prevalent threats facing the banking sector. Malware also poses a significant challenge.

Keywords: cybersecurity, cybersecurity framework, cybersecurity challenge and Cybersecurity readiness.

1. Introduction

Information technology is crucial for the success of financial organizations, offering efficient methods to collect, store, retrieve, process, transmit, and distribute data. It is seen as a competitive edge in today's work environment. The financial sector has greatly benefited from advancements in information technology, becoming increasingly reliant on it. As the volume of sensitive digital data grows rapidly, the impact of data breaches on individuals and systems also intensifies.

The banking industry, in particular, has been significantly influenced by the rapid growth of the information technology sector, making it a frequent target for IT-based attacks. Consequently, cybersecurity has become one of the primary concerns for banks.

As stated by Cisco [3], cybersecurity involves safeguarding systems, networks, and software from online threats.

Modern banking in Ethiopia began in 1905 and has seen continuous advancements up to the present. The integration of information technology services such as ATMs, Internet Banking, Mobile Banking, POS, and SMS has significantly enhanced the range of financial services available. Similar to other developed nations, Ethiopia is increasingly focusing on cybersecurity.

Ethiopian financial institutions are frequently targeted by cyberattacks, mirroring global trends. An INSA report from May 2022 highlighted an unprecedented surge in cyberattack attempts within a six-month period, predominantly targeting the banking sector. The report indicated that the Commercial Bank of Ethiopia accounted for 51% of the money lost to fraud, followed by the Bank of Abyssinia (17%), Oromia Bank (8.5%), and Wegagen Bank (8.2%). The threat landscape for financial institutions continues to grow.

According to the researcher's knowledge, there is scarcity of empirical studies in our country that assessed how prepared financial institutions are for brand-new cybersecurity challenges. Though there are some attempts there still is a need for Up-to-date empirical research to address an ever-changing threats and challenges. Therefore, this study aims to fill the research gap besides comparing the challenges posed by threats to the private and government banking sectors in Ethiopia, evaluating their readiness, Identifying the measures used by financial institutions to tackle the cybersecurity challenge, proposing ways to address recently emerging cybersecurity challenges, and developing cybersecurity a framework for the financial sector.

To address cybersecurity challenges, organizations need to pinpoint security issues to protect the confidentiality, availability, and integrity of their systems, thereby preventing asset losses from cyber-attacks. This study evaluates the cybersecurity threats faced by private and governmental institutions and examines how prepared these organizations are to tackle these challenges.

Thus, this study attempts to investigate and answer the following research questions:

- What are the challenges of cybersecurity threats on Ethiopian financial institutions?
- What readiness do Ethiopia's private and governmental financial institutions have for the challenge of cybersecurity?

2. Related Work

Agility (2022) states that the banking industry implements various measures, such as firewalls, intrusion detection systems, and encryption technologies, to safeguard their online systems and networks from cyber-attacks. The African financial sector is also vulnerable to cyber threats and incurs significant losses. However, there is a lack of tools to effectively collect, analyze, consolidate, and share data on a regional level. Consequently, breaches and losses in small or medium institutions often go unreported, as highlighted by the 11th annual EY/IIF global bank risk management survey.

According to [30], information security includes all the methods and devices enterprises use to protect data. This involves policies that prevent unauthorized access to company or personal data. The field of information security covers various topics such as network and infrastructure security, testing, and auditing, and is continually evolving. Information security aims to prevent unauthorized access, modification, or recording of sensitive data, as well as any other forms of disruption. It ensures the privacy and protection of critical data, including financial information, intellectual property, and client account details.

This research delves into recent studies on cybersecurity challenges. The first study discussed is “Assessment on Challenging Threats of Cybersecurity and its Emerging Trends on Selected Ethiopian Banking” by Bayu [8]. This article investigates the significant cybersecurity threats and emerging trends in selected financial institutions. It highlights the most prevalent cybersecurity threats in the banking sector and notes the absence of control and protective measures to mitigate these risks. Based on the study’s findings, a cybersecurity framework has been proposed to address these challenges, along with recommendations for the selected banks.

The research titled “Internet Banking Security Framework in the Case of Ethiopian Banking Industry” by Aychiluhim [13] is relevant to this study. As internet banking becomes increasingly prevalent in Ethiopian banking, cybersecurity emerges as a significant risk. The study aims to outline internet banking security and proposes a baseline architecture for the Ethiopian banking sector. It concludes that for Ethiopia to achieve the most secure internet banking channel, banks must adopt a comprehensive and integrated approach. This includes involving all key stakeholders, such as banks, consumers, authorities, and service providers, to adhere to the recommended security framework. The paper ultimately advocates for a holistic, multi-layered security approach that extends to client-side security and incorporates national financial and security intelligence teams.

Mohammed [18] conducted a study on cyber-attacks and cybersecurity readiness in Iraqi private banks. The study aimed to assess the cybersecurity preparedness of the private banking sector. Using a case study methodology and quantitative techniques, the researchers collected data primarily through a questionnaire designed based on a literature review and expert recommendations. The study did not develop a framework for cybersecurity readiness. It found that while consumers occasionally face cyber-attacks and remain concerned about them, Iraqi private banks are actively working to enhance their cybersecurity systems. The study did not suggest any further research.

The previous literature review indicates that extensive research has been conducted on related topics. Most researchers have focused on cybersecurity challenges, risks, and solutions by reviewing existing literature, without specifically examining the challenges faced by the financial sector. Only one researcher has investigated the cybersecurity threats within a single banking industry [8]. This study addresses a gap by assessing and investigating cybersecurity threats and readiness through questionnaires, in-depth interviews with bank security experts, and a review of the bank's security policy. However, there has not been a comprehensive study on the cybersecurity threats and readiness levels comparing private and governmental banking industries in Ethiopia.

3. The Proposed Solution

This paper tried to overcome cyber security issues that are a major threat for organizations information security by proposing frameworks. The proposed cyber security framework will assist the financial institutions in terms of creating cybersecurity awareness and good practices to its employees to strengthen security by mitigating vulnerabilities for attacks. The key findings are related with the two categories: cybersecurity threat challenges and the banks preparedness in tackling cybercrimes.

In the first category phishing, DDOS and social engineering are the top cyber-attacks in both government and private banks. In "email security" employees' knowledge to phishing attack links is not good. In "safely use of internet and computer" personal computers security precautions are not practiced good enough, password management is also poor. In "threats and preventive measures" respondent security practices are below average. For instance, updating software, antivirus usage, security scanning and backup are not performed regularly in a timely manner. In "password management and security" respondents‟ password setting, changing and protection practices are unsatisfactory. In "information security terms and social engineering" section respondents‟ knowledge to information security responsibility and social engineering needs improvement. In "security standards, procedures and training" section the organization doesn't use information security standards, doesn't has well-organized procedures in case of cyber-attacks and employees are not being trained of information security. In "firewall, IPS, penetration and traffic control" the organization is not performing internal and external penetration testing. The implementation and usage of IPS/IDS and web filtering is unsatisfactory. In "wireless network security" the organization wireless network implementation and security management are not good. In the rest six sections multiple

security features are not implemented enough to strengthen the organization security posture such as port-based filtering, enabling port security, disabling unused ports etc. Ignoring these important issues may cause vulnerabilities to multiple cyber-attacks such as denial of service attacks and a business down time which is unacceptable to a financial institution. Overall the employees‟ information security awareness is not satisfactory and needs to be dealt with such kind of programs to protect its assets or even its business. Open line communication between financial institutions is also poor hence knowledge base systems is mandatory. Any platform either from information security administration (INSA) or national bank is encouraged.

This study is proposed in order to study and identify the challenges and preparedness in private and government banks. To secure the financial institutions assets there is a need for appropriate framework for organizations based on their context. NIST framework (2017) stated that the framework is not a one-size-fit all approach to managing Cybersecurity risks for information assets.

According to Hevner (2004), in order to validate the research, design science research relies on a thorough examination and re-construction of the design artifact contributions as described in the fourth principle. The suggested framework is examined in two rounds even if it is not thoroughly tested. With the chosen cyber specialists, a focus group discussion served as the initial phase of expert validation. The initial draft framework's completeness, correctness, and clarity were to be discussed, along with any room for improvement, during the focus group discussion. Individual conversations with the experts were then held to have a thorough discussion and get more comments. The proposed framework was updated to increase its completeness, clarity, and accuracy in response to the experts' feedback.

After the proposed framework was changed, a second round of expert validation was carried out using the survey to collect individual opinions on the revised framework's completeness, clarity, and correctness. During this stage, additional IT division staff members were invited to take part in the survey by briefly outlining the suggested framework.

The Hevener (2004) evaluation criteria, which include fit to the organization, comprehensiveness, reliability, clarity, correctness, and usability quality attributes, served as the basis for the questionnaire's content.

Finally, the abellow cybersecurity framework was developed by associating the findings of the research associating with NIST frameworks.

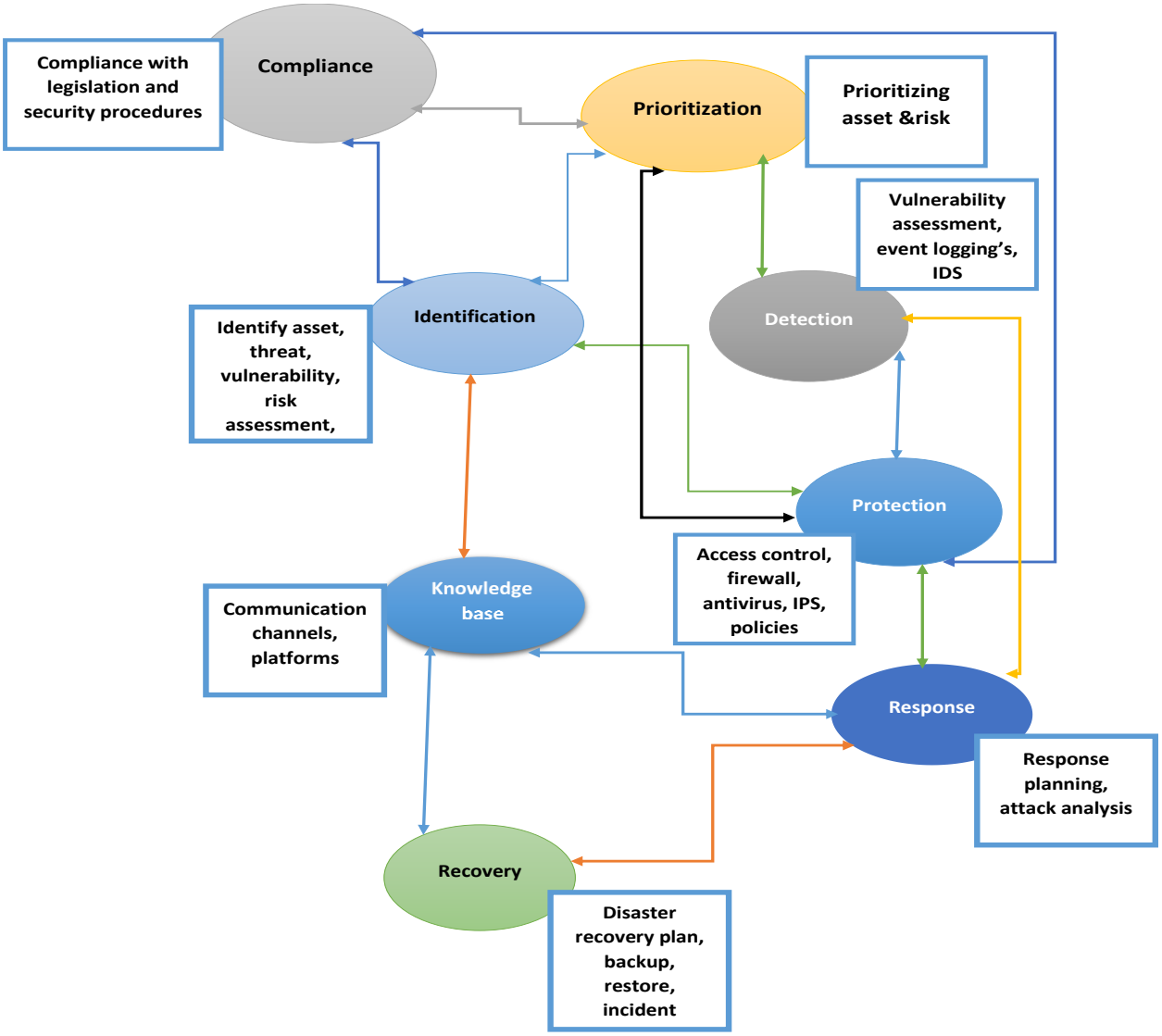

Figure 1. The proposed cybersecurity framework

4. Conclusion and Future Work

In order to customize a cybersecurity framework, this research examines cybersecurity challenges and readiness at private and government banks. Based on this research, the findings showed that social engineering, phishing and Distributed denial of service (DDOS) attacks are mentioned as the most security challenge in both private and government financial institutions. On the other hand, session high jacking attack is less visible too. Hence, special attention should be given on the three types of cyber-attacks. In order to alleviate and combat security issues, classification of those challenges should be important. Topics related to potential cybersecurity challenge, occurrence of cybersecurity challenge, cybersecurity policy and procedures, man power and capacity building, banks cooperation with other financial institutions and availability and use of cybersecurity infrastructures solutions are deeply discussed. In order to identify the challenges and difficulties of cybersecurity at selected private and government banks,

framework was developed in combination with NIST frame work Core process, specifically identify, detect, prevent, respond, and recover.

The study's analysis and results led to the following five conclusions, which are listed below:

- Lack of well-prepared vital infrastructures like web gateway and filtering solutions; disaster recovery sites, email filtering gateway is clearly seen.
- Lack of internal experience, bad leadership skill, lack of dedicated security teams are the issues related with challenges existed. Similar issues with inadequate funding, poor open line communications contribute to the sever security issues.
- The study found that attacks like phishing, DDOS and social engineering the most security challenge of both private and government banks.
- The study found that the challenges lacked effective defenses against insider risks since most of the cybersecurity issues arises from insider.
- Although there were challenges in the financial institutions, the banks are at the high preparedness level in order to combat the growing risk of cybersecurity.

The research's results and conclusions highlight the issues, growing trends, and level of preparation for cybersecurity as well as any important cyber threats or exposure.

This research proposed a conceptualized framework that is used to guide the financial institutions to safeguard their information assets. The future scholar wider the scope to incorporate all Government and private institutions to have a generic cyber security framework Considering new technologies and infrastructures. In addition, the researcher will consider developing a knowledge base system for cyber security solutions.

References

[1] Selgin and G. A, "Encyclopedia Britannica," 6 April 2022. [Online]. Available: https://www.britannica.com/topic/bank.

[2] Afi, "CYBERSECURITY FOR FINANCIAL," October 2019.

[3] Cisco, "Cisco.com," 2022. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~types-of-threats.

[4] S. &. S. N. &. M. S. P.S, "Overview of Cyber Security," IJARCCE, vol. 7, pp. 125-128, 2018.

[5] A. MAURI, "MyIDEAS," Departmental Working Papers, 04 2003. [Online]. Available: <https://ideas.repec.org/p/mil/wpdepa/2008-11.html> .

[6] K. Adane, "SSRN," Arba Minch University, 1 September 2020. [Online]. Available: https://ssrn.com/abstract=3545189.

[7] C. P. S. Technologies, "Linkedin," 26 November 2022. [Online]. Available: https://www.linkedin.com/showcase/check-point-software-africa/?originalSubdomain=za.

[8] B. Gezahegn, "Assessment on Challenging Threats of Cyber Security and its Emerging trends on Selected Ethiopian Banking," 2020.

[9] T. Shimels, "Maturity of Information System Security In Selected Priavte banks in Ethiopia," 2021.

[10] K. Markos, "Factors influencing information security investements in the Ethiopian Bankig sector," 2022.

[11] B. Wedelu, "Information and Cyber Security Risk Assessment Framework for the Banking Sector in Ethiopia," 2017.

[12] B. G. Mawudo, M.-H. Kim and B. G. Mawudor, "Continuous Monitoring Methods as a Mechanism forDetection and Mitigation of Growing Threats in Banking Security System," 2015.

[13] A. Desisa, "Internet Banking Security Framework: The case of Ethiopian Banking Industry," 2014.

[14] R. Chatterjee, "CIM," 5 MARCH 2020. [Online]. Available: https://analyticsindiamag.com/difference-between-cybersecurity-information-security/.

[15] Kaspersky, "Kaspersky," 2022. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

[16] NIST, "NIST COMPUTER SECURITY RESOURCE CENTER," 2013. [Online]. Available: https://csrc.nist.gov/glossary/term/cybersecurity.

[17] A. O. N. B. A. Obotivere, "Cyber Security Threats on the Internet and Possible Solutions," International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, 9, September 2020.

[18] M. F. Hasan, "Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case," Rsearchgeat, August 2021.

[19] M. Stamp, Information security:, 2011.

[20] . S. C. B. J. H. D. E. G. B. T. W. C. and C. M. , "Botnets: The Killer Web Applications," Elsevier, 2007.

[21] M. H. "google," 2007. [Online]. Available: http://books.google.com.my/books?id=MDzio.

[22] CISA, "Cyber security and Infrastracture security Agency," 20 November 2019. [Online]. Available: https://www.cisa.gov/uscert/ncas/tips/ST04-015.

[23] Redhat, "www.redhat.com," 30 September 2022 . [Online]. Available: https://www.redhat.com/en/topics/security/software-development-lifecycle-security.

[24] Vmware, "Modern Bank Heists 4.0," 2021. [Online]. Available: https://www.vmware.com/learn/security/modern-bank-heists-2021.html.

[25] J. M. B. a. F. T. Chong, "Emerging Technologies for Quantum Computing," vol. vol. 41, pp. pp. 41-47, Sept.-Oct. 2021, .

[26] Techtarget, "Techtarget," [Online]. Available: https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.

[27] S. Scorecard, "Security Scorecard," 07 12 2021. [Online]. Available: https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation/.

[28] E. Taddele, "ERP Post-Implementation Management Framework: The case of," Addis Ababa University, June 2015.

[29] M. Velychko, "Conceptual Framework in Research," 2019.

[30] Imperva, "Imperva," 2021. [Online]. Available: https://www.imperva.com/blog/2021-in-review-part-1-5-cybersecurity-topics-that-made-news/.

[31] K. Noor, "Case Study: A Strategic Research Methodology: Universiti Industri Selangor," Shah Alam, pp. 1602-1904, 2008.

[32] I. Akhtar, "Research Design," Social research foundation, September 2016.

[33] T. Boru, "Mitigating cyber threats to banking industry," Universiti Utara Malaysia, 2018.

[34] S. McCombes, "Correlational Research," [Online]. Available: https://www.scribbr.com/methodology/correlational-research. [Accessed 2019].

[35] M. Given, "The SAGE Encyclopedia of Qualitative Research Methods," SAGE Publications, 2008.

[36] Vedantu, "Vedantu," 2022. [Online]. Available: https://www.vedantu.com/commerce/census-and-sample-survey.

[37] Simplilearn, "Simplilearn," 22 November 2022. [Online]. Available: https://www.simplilearn.com/what-is-data-collection-article.