International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

A Comparative Analysis of Different Cyber Security Frameworks and Their Effectiveness in Mitigating Cyber Threats a Case Study of Union Bank Jaba Local Government Area of Kaduna State

Christopher Patrick[1], Ezekiel Friday[2]
Department of Information Technology Management[1], Department of Management Science[2], Global Wealth University Lome, Togo[1], Joint Professional Training and Support International Lagos, Nigeria[2]

Date of Submission: 13-06-2024 Date of Acceptance: 27-06-2024

ABSTRACT
This study was carried out on A comparative analysis of different cyber security frameworks and their effectiveness in mitigating cyber threats. A case study of union bank Jaba local government area of Kaduna state. To achieve this objective, the researcher developed and administered a questionnaire on Twenty eight staff of Union bank Kwoi in Jaba Local Government Area of Kaduna State. The T-test was used in testing the null hypothesis. From the study, it shows that the current cybersecurity framework implemented at Union Bank is highly effective in mitigating cyber threats. It shows that the cybersecurity framework used at Union Bank is easy to implement and manage. This study shows that Employees at Union Bank are adequately trained and aware of the cybersecurity framework in place. This study shows Union Bank's cybersecurity framework allows for a quick and effective response to cyber threats. This study shows that the cybersecurity framework used at Union Bank complies with industry standards and best practices. It was observed that Since the implementation of the current cybersecurity framework, Union Bank's overall security posture has improved significantly. It was observed that Users at Union Bank are satisfied with the cybersecurity measures currently in place. The study recommends, Union Bank should consider adopting a hybrid approach that leverages the strengths of NIST, ISO/IEC 27001, and COBIT. This integration can offer a more comprehensive and flexible cybersecurity strategy that addresses the diverse and evolving nature of cyber threats. Implement continuous monitoring mechanisms to regularly assess the effectiveness of the adopted cybersecurity measures. This will help in identifying and mitigating new threats promptly. Conduct regular cybersecurity training and awareness programs for all employees. Human error remains a significant vulnerability in cybersecurity, and well-informed staff are the first line of defense against cyber threats. Invest in advanced cybersecurity technologies such as AI and machine learning for threat detection and response. These technologies can enhance the bank's ability to detect and respond to sophisticated cyber threats in real-time. Conduct regular audits and compliance checks to ensure that all cybersecurity measures are up to date and in line with current standards and regulations. This will help in maintaining the integrity and security of the bank's information systems. Regularly consult with cybersecurity experts and industry professionals to stay updated on the latest threats and best practices. This can provide valuable insights and guidance for enhancing the bank's cybersecurity posture.

Keywords: **Cybersecurity, Cyber Security Frameworks**, **Comparative Analysis**, **Effectiveness**, **Mitigating Cyber Threats.**

I. INTRODUCTION

Cyber security came about as a result of advances in information and communication technology (ICT). The cyber security threats became pronounced in Africa from 2007 through reading the attacks from Eastern Europe. Furthermore, the failure to deal with threats emerging from the cyber space was compounded by the fact that, in several states there were no proper definitions of functions, institutions, resources and skills. Consequently, the cyber security resilience can be achieved through the "national cyber security strategy" as was later developed by [10]. Cyber security is a menace of serious concern to the nation, Nigeria. Due to its national priority, it is now handled by the President's office. The President of Nigeria through his National Security Adviser in 2016 consented to the country's bill on Cyber Crime. The drafts on Nigeria cyber security policy and strategy were

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

officially. In June, 2017, the National Cyber Security Policy and Strategy drafts were officially unveiled in 2017 in Lagos at a seminar [14].

In recent years, the proliferation of cyber threats has posed significant challenges to organizations across various sectors include the banking sector. Cybersecurity frameworks play a crucial role in helping organizations establish robust defense mechanisms against these threats. This study aims to conduct a comparative analysis of different cybersecurity frameworks to evaluate their effectiveness in mitigating cyber threats.

Cybersecurity frameworks provide structured guidelines and best practices for organizations to manage and mitigate cybersecurity risks effectively [13]. By implementing these frameworks, organizations can enhance their resilience against cyber threats and ensure the confidentiality, integrity, and availability of their critical assets [9].

According to [16] In today's interconnected world, where technology plays a pivotal role in our daily lives, the concept of cybersecurity has become more crucial than ever. Cybersecurity frameworks serve as structured guidelines & best practices designed to safeguard digital systems, networks & data from potential threats & vulnerabilities. These Cybersecurity Frameworks provide a systematic approach to managing & mitigating cyber risks, ensuring the Confidentiality, Integrity & Availability [CIA] of information.

The digital age has ushered in unprecedented advancements, transforming the way we communicate, work & conduct business. While these technological leaps bring countless benefits, they also expose us to new evolving cyber threats. The importance of cybersecurity lies in its ability to fortify our defences against malicious actors seeking unauthorized access, data breaches & disruption of critical systems. As our reliance on digital technologies continues to grow, so does the significance of implementing robust cybersecurity measures to protect sensitive information ensure the smooth functioning of digital ecosystems.

The purpose of conducting a comparative analysis of Cybersecurity Frameworks is to evaluate & understand the strengths, weaknesses & unique features of different approaches. By comparing various Cybersecurity Frameworks organisations can make informed decisions about which one aligns best with their specific needs, operational context & risk tolerance. This analysis aids in the selection of a Cybersecurity Frameworks that not only comply with industry standards but also addresses the specific challenges & requirements of an organisation. Additionally, these Cybersecurity Frameworks help in identifying gaps or overlaps in existing frameworks, enabling the development of a comprehensive & effective cybersecurity strategy.

With the rapidly increasing prominence of information technology in recent decades,various types of security incidents, such as unauthorized access [11], denial of service (DoS) [18], malware attack [12], zero-day attacks [1], data breaches [17], social engineering or phishing [7], etc., have increased at an exponential rate in the last decade. In 2010, the security community documented less than 50 million distinct malware executables. In the year 2012, this reported number doubled to around 100 million. From the record according to AV-TEST statistics, the security industry detected over 900 million malicious executables in 2019, and this number is rising [5]. Cybercrime and network attacks can result in significant financial losses for businesses and people. For example, according to estimates, an average data breach costs USD 3.9 million in the United States and USD 8.19 million globally [3], and cybercrime costs the world economy USD 400 billion per year. The security community estimates [4] , over the next five years, that the number of records broken will nearly quadruple. As a result, to minimize further losses, businesses must create and implement a comprehensive cybersecurity strategy. The most recent socioeconomic studies show that [15] the nation's security is dependent on governments, people with access to data, applications and tools that require high security clearance.

It is also dependent on businesses that give access to their employees, who possess the capacity and knowledge to identify such cyber-threats quickly and effectively. As a result, the primary concern that must be addressed immediately is to intelligently identify various cyber occurrences, whether previously known or unseen, and safeguard critical systems from such cyber-attacks adequately Cybersecurity refers to technologies and techniques that protect programs, networks, computers and data from being damaged, attacked or accessed by unauthorized people. Cyber security covers various situations, from corporate to mobile computing, and can be divided into several areas. These are:

1. network security, which focuses on preventing cyber-attackers or intruders from gaining access to a computer network;

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

2. application security, which considers keeping devices and software free of risks or cyber-threats;
3. information security, which primarily considers the security and privacy of relevant data; and
4. operational security refers to the procedures for handling and safeguarding data assets. Traditional cybersecurity solutions include a firewall, antivirus software or an intrusion detection system in network and computer security systems. Data science is driving the transformation, where machine learning, an essential aspect of "Artificial Intelligence", can play a vital role in discovering hidden patterns from data. Data science is pioneering a new scientific paradigm, and machine learning has substantially impacted the cybersecurity landscape [19], [2]. As discussed in the article Cost of Cyber Attacks vs. Cost of Cybersecurity in 2021, with the advancement of technologies pertinent to launching cyber threats, attackers are becoming more efficient, giving rise to an increasing number of connected technologies.

1.2 EFFECTIVELY MITIGATING CYBER THREATS

Effectively mitigating cyber threats involves a multi-faceted approach that combines technology, processes, and human expertise. Here are several strategies and practices commonly employed:

1. Risk Assessment and Management: Regularly assess and prioritize cybersecurity risks to understand potential threats and their potential impact on the organization. Implement risk management processes to prioritize mitigation efforts.
2. Security Awareness Training: Educate employees about common cyber threats, such as phishing attacks and social engineering, to help them recognize and respond appropriately to potential risks.
3. Strong Authentication Mechanisms: Implement multi-factor authentication (MFA) and strong password policies to enhance access controls and prevent unauthorized access to sensitive systems and data.
4. Patch Management: Keep software and systems up to date with the latest security patches and updates to address known vulnerabilities and reduce the attack surface.
5. Network Segmentation: Segregate networks and systems to limit the spread of cyber threats in case of a breach and to protect critical assets from unauthorized access.
6. Endpoint Security: Deploy endpoint protection solutions, such as antivirus software and endpoint detection and response (EDR) tools, to detect and mitigate threats targeting end-user devices.
7. Firewalls and Intrusion Detection/Prevention Systems: Implement firewalls and intrusion detection/prevention systems to monitor and control network traffic, detect malicious activities, and block or mitigate threats in real-time.
8. Data Encryption: Encrypt sensitive data both at rest and in transit to protect it from unauthorized access and mitigate the impact of data breaches.
9. Incident Response Planning: Develop and regularly test incident response plans to ensure a timely and effective response to cybersecurity incidents, minimizing their impact on the organization.
10. Continuous Monitoring and Threat Intelligence: Monitor networks and systems continuously for signs of malicious activity and leverage threat intelligence feeds to stay informed about emerging cyber threats and tactics used by threat actors.
11. Vendor Risk Management: Assess and manage the cybersecurity risks associated with third-party vendors and partners who have access to your systems or handle sensitive data.
12. Regulatory Compliance: Ensure compliance with relevant cybersecurity regulations and standards to mitigate legal and regulatory risks associated with data breaches and cyber incidents.
13. Cybersecurity Awareness Programs: Foster a culture of cybersecurity awareness within the organization by promoting best practices, encouraging reporting of suspicious activities, and rewarding positive security behaviors.
14. Regular Security Audits and Penetration Testing: Conduct regular security audits and penetration testing to identify and address vulnerabilities before they can be exploited by threat actors.
15. Cyber Insurance: Consider purchasing cyber insurance to help mitigate financial losses associated with data breaches and cyber incidents that cannot be fully prevented.

By implementing a combination of these strategies and continually adapting to evolving cyber threats, organizations can enhance their resilience to cyber attacks and better protect their assets and sensitive information

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

II. RESEARCH DESIGN (DESCRIPTIVE)

Research design is the framework of research methods and techniques chosen by a researcher. The design allows researchers to hone in on research methods that are suitable for the subject matter and set up their studies up for success, in this research descriptive design will be consider over other research design.

In a descriptive design, a researcher is solely interested in describing the situation or case under their research study. It is a theory-based design method which is created by gathering, analyzing, and presenting collected data. This allows a researcher to provide insights into the why and how of research. Descriptive design helps others better understand the need for the research. If the problem statement is not clear, you can conduct exploratory research.

A research design is the structure of research. It holds all the elements in a research project together. It shows how all the major parts of the research project work together to try to address the central research question.

2.1 DATA COLLECTION PROCEDURE

For the purpose of this research work, the researcher used the questionnaire, which is a structured series of questions in written form meant to be answered by respondents. The question forms are to be either ticked or choose by those concerned. The researcher issued questions to staff of union bank Kwoi, Jaba local government area of Kaduna state

The questionnaires for staff were mainly issued to obtained information.

2.2 TARGET POPULATION

The Population of this study comprises of members staff of Union bank Plc Kwoi branch in Jaba Local Government Area of Kaduna state. This includes the full and contract staff, and other staff. Comprising of 28 in all

2.3 METHOD OF DATA ANALYSIS

In order to facilitate the execution of this research work, certain forms of data were utilized they are primary and secondary data.

2.4 RESEARCH INSTRUMENTATION

In choosing stated research instrument, the researcher takes into consideration the nature and scope of the research study, the structure and activities and the convenience associated with cost.

The researcher administered questionnaires on the quest to obtain information.

2.5 SAMPLING TECHNIQUE

The technique used in this research work is Random sampling technique. This method enabled the researcher to select a sample from population so that each member have equal chance of being selected.

2.6 ANALYTICAL TOOL

The analytical tool use in this research is T-test method.

In order to analyze the data, the methodology used is likert Scale method, (Statistical and graphical method). Ordinary, data in this form are unbiased. Is the most widely employed form of attitude measurement in Survey research? The likert scale is a special type of the more general class of summated rating scale constructed from multiple ordered – category items.

Each item uses a set of symmetrically balanced bipolar response categories indicating varying levels of agreement or disagreement with a specific stimulus statement expressing an attitude or opinion.

III. ANALYSIS OF DATA AND DISCUSSION OF RESULT FINDINGS

Data is collected through survey method [8]. This is original in nature. This data is collected by distributing the questionnaire and getting filled by the concerned respondents and personal interview.

Questionnaire used for survey consist questions based on Likert scale. Likert scale is used to balance on both the side of neutral option. Likert Scale [8] and [6] is used because one of standard scale to collect opinion experiences or specific data.

1. The current cybersecurity framework implemented at Union Bank is highly effective in mitigating cyber threats.

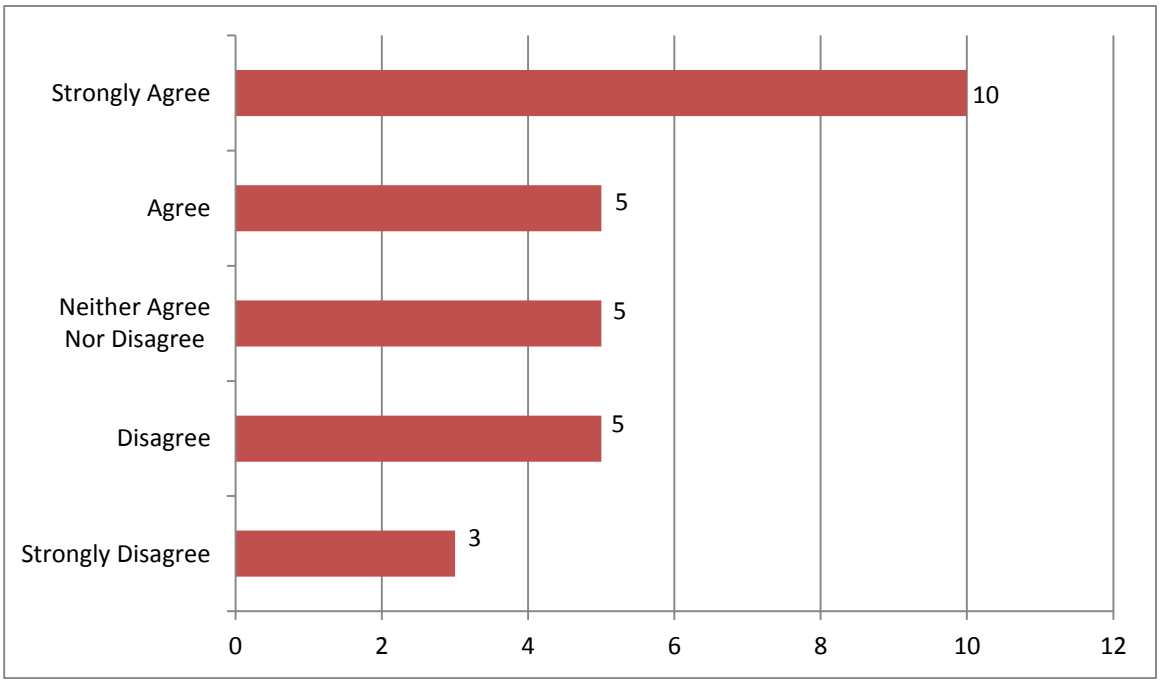
International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

Table 3.1 the current cybersecurity framework implemented at Union Bank is highly effective in mitigating cyber threats.

The current cybersecurity framework implemented at Union Bank is highly effective in mitigating cyber threats.	**SA**	**A**	**N**	**DA**	**SD**	**TOTAL**
No. of Response	10	5	5	5	3	28
Percentage of Response	36%	18%	18%	18%	10%	100%
Source: Field Survey 2024						

Table 3.1.Of the total 28 respondents, 54% respondents agree or strongly agree that the current cybersecurity framework implemented at Union Bank is highly effective in mitigating cyber threats, 18% neither agree nor disagree and 28% disagree or strongly disagree.

Chart 3.1: Response to likert scale shows that the current cybersecurity framework implemented at Union Bank is highly effective in mitigating cyber threats.



2. The cybersecurity framework used at Union Bank is easy to implement and manage."

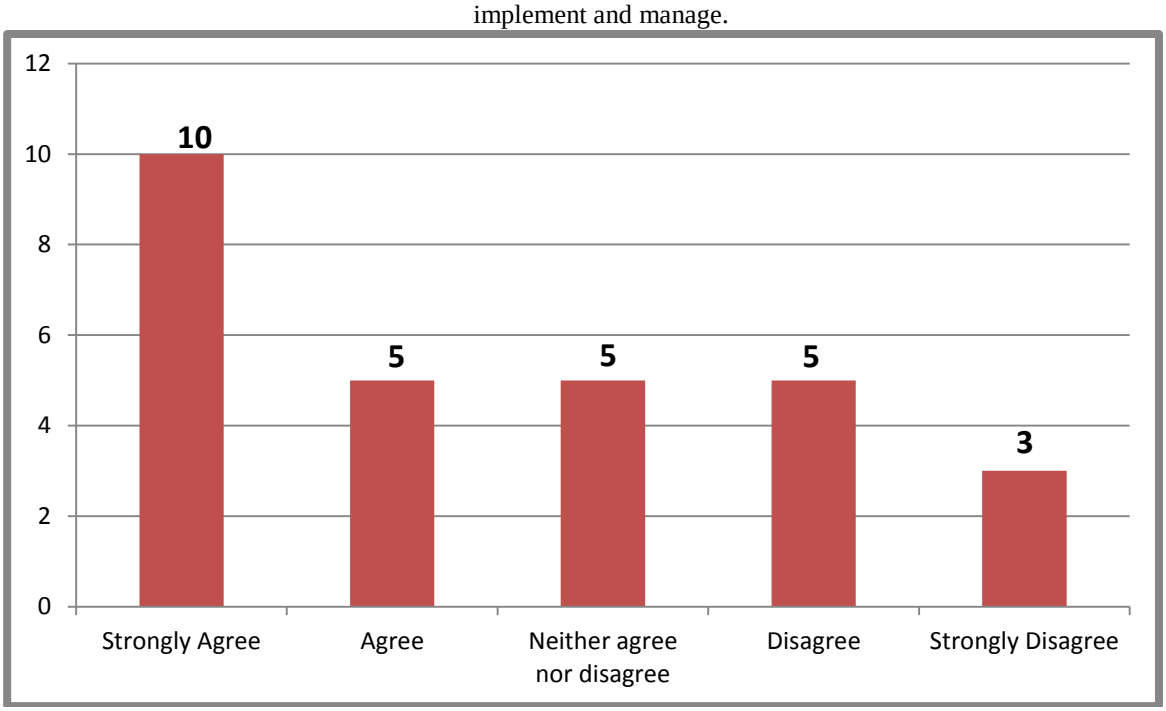
Table 3.2: The cybersecurity framework used at Union Bank is easy to implement and manage.

The cybersecurity framework used at Union Bank is easy to implement and manage	**SA**	**A**	**N**	**DA**	**SD**	**TOTAL**
No. of Response	10	5	5	5	3	28
Percentage of Response	36%	18%	18%	18%	10%	100
Source: Field Survey 2024						

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

Table 3.2: Of the total 28 respondents, 54% respondents agree or strongly agree that the cybersecurity framework used at Union Bank is easy to implement and manage, 18% neither agree nor disagree and 28% disagree or strongly disagree.

Chart 3.2: Response to likert scale shows that the cybersecurity framework used at Union Bank is easy to implement and manage.



3. Employees at Union Bank are adequately trained and aware of the cybersecurity framework in place.

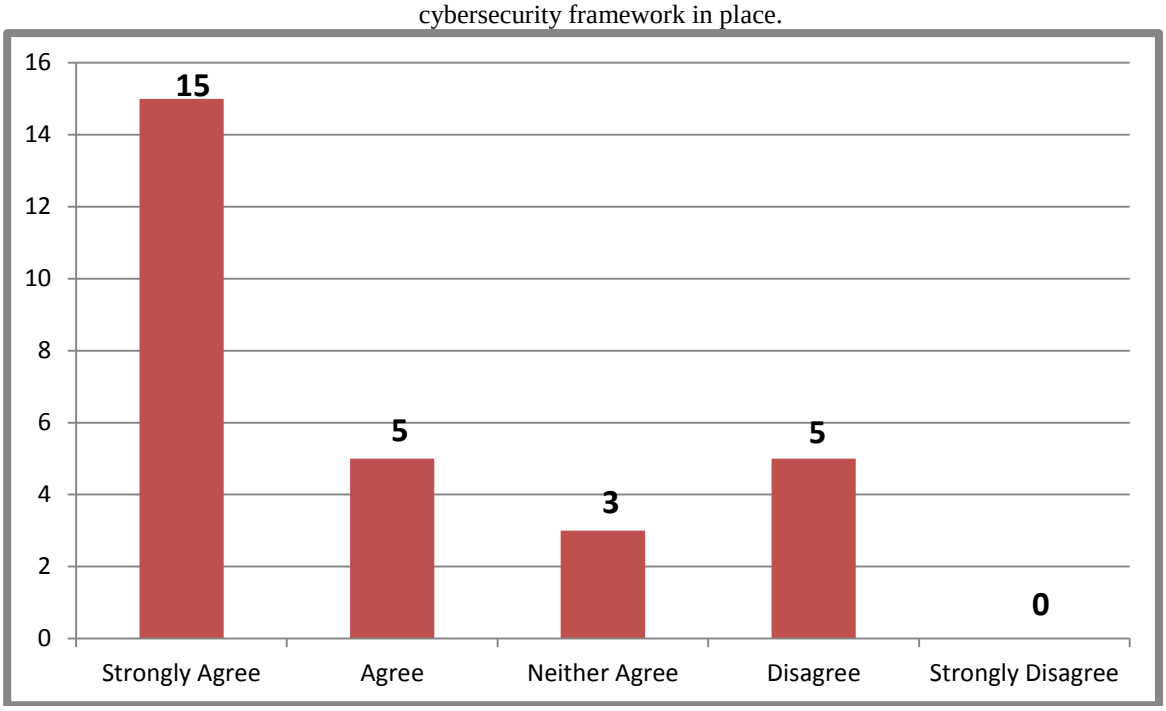
Tables 3.3Employees at Union Bank are adequately trained and aware of the cybersecurity framework in place.

Employees at Union Bank are adequately trained and aware of the cybersecurity framework in place.	**SA**	**A**	**N**	**DA**	**SD**	**TOTAL**
No. of Response	15	5	3	5	0	28
Percentage of Response	54%	18%	10%	18%	0%	100
Source: Field Survey 2024						

Table 3.3: Of the total 28 respondents, 72% respondents agree or strongly agree that Employees at Union Bank are adequately trained and aware of the cybersecurity framework in place, 10% neither agree nor disagree and 18% disagree or strongly disagree.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

Chart 3.3: Response to likert scale shows that Employees at Union Bank are adequately trained and aware of the cybersecurity framework in place.



4. Union Bank's cybersecurity framework allows for a quick and effective response to cyber threats

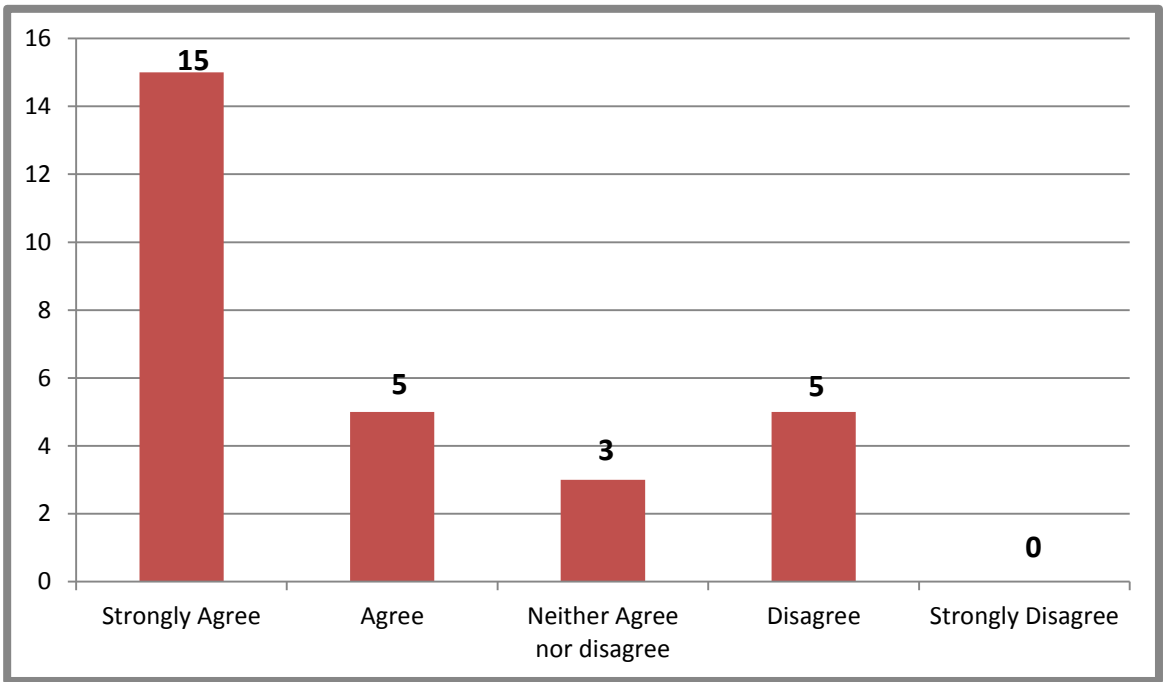
Table 3.4: Union Bank's cybersecurity framework allows for a quick and effective response to cyber threats.

Union Bank's cybersecurity framework allows for a quick and effective response to cyber threats	**SA**	**A**	**N**	**DA**	**SD**	**TOTAL**
No. of Response	15	5	3	5	0	28
Percentage of Response	54%	18%	10%	18%	0%	100
Source: Field Survey 2024						

Table 3.4: Out of the total 28 respondents, 72% respondents agree or strongly agree Union Bank's cybersecurity framework allows for a quick and effective response to cyber threats, 10% neither agree nor disagree and 18% disagree or strongly disagree.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

Chart 3.4: Response to likert scale shows Union Bank's cybersecurity framework allows for a quick and effective response to cyber threats.



5. The cybersecurity framework used at Union Bank complies with industry standards and best practices.

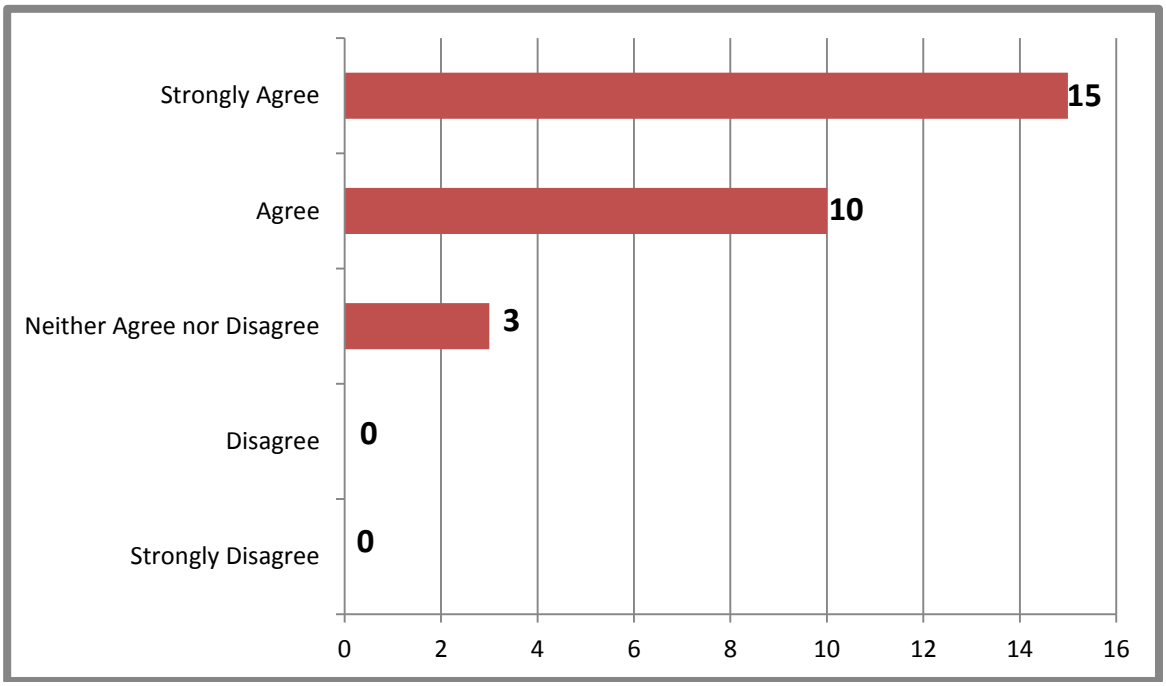
Table 3.5: The cybersecurity framework used at Union Bank complies with industry standards and best practices.

neighborhood have influence on the academic performance of secondary school students	**SA**	**A**	**N**	**DA**	**SD**	**TOTAL**
No. of Response	15	10	3	0	0	28
Percentage of Response	54%	36%	10%	0%	0%	100
Source: Field Survey 2024						

Table 3.5: Out of the total 28 respondents, the above table shows that 90% respondents agree or strongly agree that the cybersecurity framework used at Union Bank complies with industry standards and best practices, 10% neither agree nor disagree and 0% disagree or strongly disagree.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

Chart 3.5: Response to likert scale shows that the cybersecurity framework used at Union Bank complies with industry standards and best practices.



6. Since the implementation of the current cybersecurity framework, Union Bank's overall security posture has improved significantly.

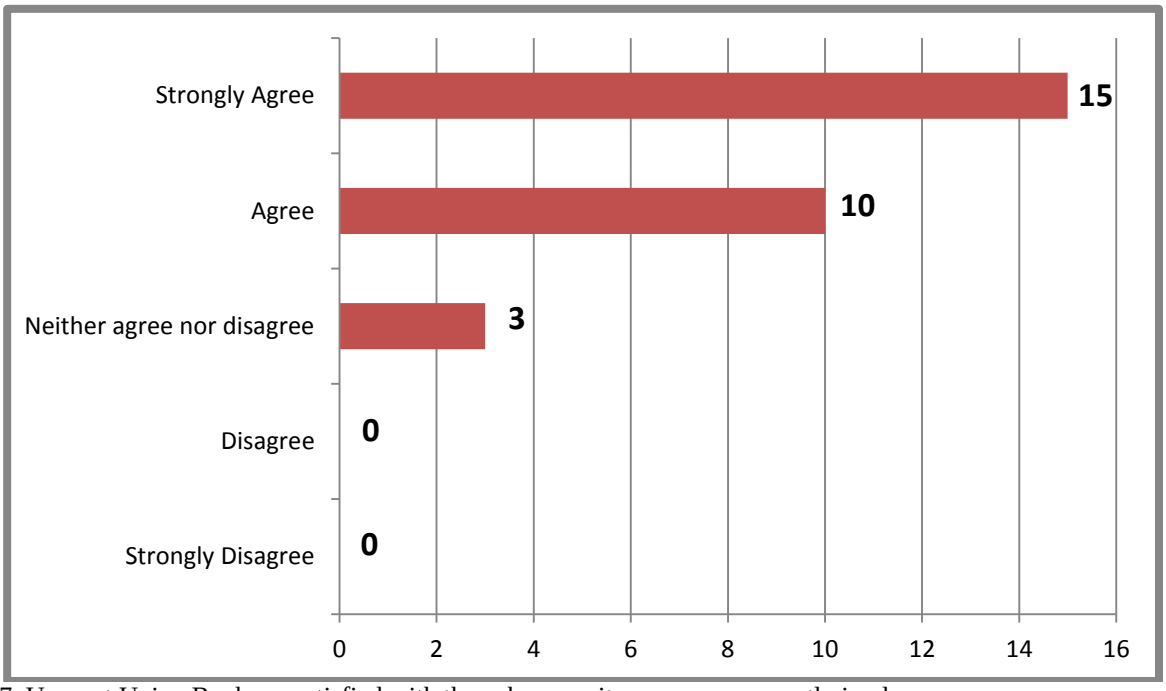
Table 3.6 Since the implementation of the current cybersecurity framework, Union Bank's overall security posture has improved significantly.

Since the implementation of the current cybersecurity framework, Union Bank's overall security posture has improved significantly.	**SA**	**A**	**N**	**DA**	**SD**	**TOTAL**
No. of Response	15	10	3	0	0	28
Percentage of Response	54%	36%	10%	0%	0%	100
Source: Field Survey2024						

Table 3.6 .Out of the total of 28 respondents, 90% respondents agree or strongly agree that Since the implementation of the current cybersecurity framework, Union Bank's overall security posture has improved significantly, 10% neither agree nor disagree and 0% disagree or strongly disagree.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

Chart 3.6: Response to likert scale shows Since the implementation of the current cybersecurity framework, Union Bank's overall security posture has improved significantly.



7. Users at Union Bank are satisfied with the cybersecurity measures currently in place.

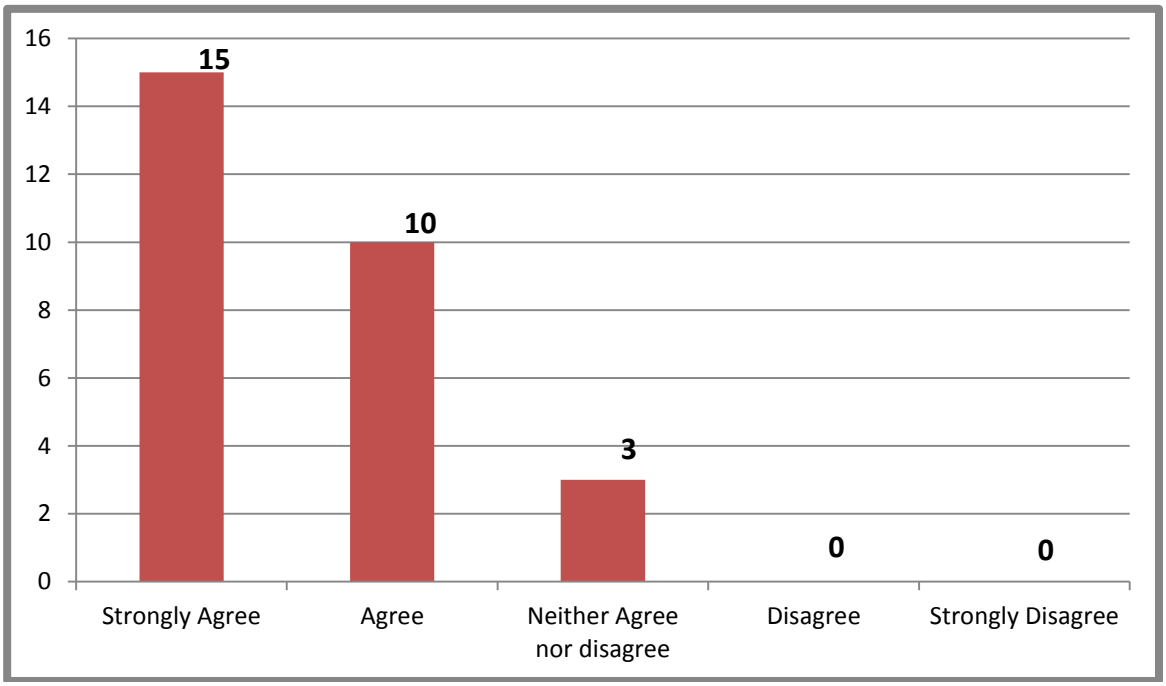
Table 3.7. Users at Union Bank are satisfied with the cybersecurity measures currently in place.

Users at Union Bank are satisfied with the cybersecurity measures currently in place.	**SA**	**A**	**N**	**DA**	**SD**	**TOTAL**
No. of Response	15	10	3	0	0	28
Percentage of Response	54%	36%	10%	0%	0%	100
Source: Field Survey 2024						

Table 3.7: Out of the total of 28 respondents, 90% respondents agree or strongly agree that Users at Union Bank are satisfied with the cybersecurity measures currently in place, 10% neither agree nor disagree and 0% disagree or strongly disagree.

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 4, Issue 3, May.-June, 2024, pp: 1663-1674 www.ijhssm.org

Chart 3.7: Response to likert scale shows that Users at Union Bank are satisfied with the cybersecurity measures currently in place.



IV. CONCLUSION

The study set out to examine A comparative analysis of different cyber security frameworks and their effectiveness in mitigating cyber threats. A case study of union bank Jaba local government area of Kaduna state:

In conclusion, the comparative analysis of various cybersecurity frameworks demonstrates their varying degrees of effectiveness in mitigating cyber threats, with specific emphasis on their application within Union Bank in Jaba Local Government Area of Kaduna State. The study reveals that while frameworks such as NIST, ISO/IEC 27001, and COBIT provide robust guidelines and practices, their effectiveness is highly contingent upon the bank's commitment to implementation and continuous monitoring. Union Bank's adoption of a comprehensive and adaptable cybersecurity framework, integrating best practices from multiple standards, has proven essential in addressing the dynamic and complex nature of cyber threats. Therefore, a multi-faceted approach tailored to the unique operational context and threat landscape of the bank significantly enhances its cyber resilience. This case study underscores the importance of not only selecting an appropriate framework but also ensuring rigorous adherence and adaptive improvement to safeguard against evolving cyber risks.

REFERENCES

[1]. Alazab, M.; Venkatraman, S.;Watters, P.; Alazab, M. 2011. Zero-day malware detection based on supervised learning algorithms of API call signatures. In Proceedings of the Ninth Australasian Data Mining Conference (AusDM'11), Ballarat, Australia, 1–2 December 2011.

[2]. Benioff, M. 2010. Data, data everywhere: A special report on managing information (pp. 21–55). The Economist, 27 February 2010.

[3]. Buecker, A.; Borrett, M.; Lorenz, C.; Powers, C, 2010. Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security; International Technical Support Organization: Riyadh, Saudi Arabia, 2010.

[4]. Chernenko, E.; Demidov, O.; Lukyanov, F, 2018. Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms; Council on Foreign Relations: New York, NY, USA, 2018.

[5]. Geer, D.; Jardine, E.; Leverett, E, 2020. On market concentration and cybersecurity risk. J. Cyber Policy 2020, 5, 9–29. [CrossRef]

[6]. Geoff Norman, (2010). "Likert Scales, levels of measurement and the laws of statistics," Sponger science Biz media B.V.
[7]. Gupta, B.B.; Tewari, A.; Jain, A.K.; Agrawal, D.P, 2017. Fighting against phishing attacks: State of the art and future challenges. Neural Comput. Appl. 2017, 28, 3629–3654. [CrossRef]
[8]. Harry, N.B, and Deborah A.B (2012) "analyzing likert data,"
[9]. International Organization for Standardization (ISO). (2019). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.
[10]. Kelly, J.: Strategic perspectives on cyber-security management and public policies. European Cyber-security Journal, 2016, 1(1): 26-72
[11]. Li, S.; Da Xu, L.; Zhao, S. The internet of things: A survey. Inf. Syst. Front. 2015, 17, 243–259. [CrossRef]
[12]. McIntosh, T.; Jang-Jaccard, J.; Watters, P.; Susnjak, T. 2019. the inadequacy of entropy-based ransomware detection. In Proceedings of the International Conference on Neural Information Processing, Sydney, Australia, 12–15 December 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 181–189.
[13]. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov/cyberframework
[14]. Osho, O. and Onoja, A. D.: National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology, 2017, 9 (1): 120 – 143.
[15]. Papastergiou, S.; Mouratidis, H.; Kalogeraki, E.M 2019. Cyber security incident handling, warning and response system for the european critical information infrastructures (cybersane). In Proceedings of the International Conference on Engineering Applications of Neural Networks, Crete, Greece, 24–26 May 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 476–487.
[16]. Retrieved from https://www.neumetric.com/comparative-analysis-of-cybersecurity-frameworks/
[17]. Shaw, A. 2009. Data breach: From notification to prevention using PCI DSS. Colum. JL Soc. Probs. 2009, 43, 517.
[18]. Sun, N.; Zhang, J.; Rimba, P.; Gao, S.; Zhang, L.Y.; Xiang, Y. 2018 Data-driven cybersecurity incident prediction: A survey. IEEE Commun. Surv. Tutor. 2018, 21, 1744–1772. [CrossRef]
[19]. Tolle, K.M.; Tansley, D.S.W.; Hey, A.J, 2011. The fourth paradigm: Data-intensive scientific discovery [point of view]. Proc. IEEE 2011, 99, 1334–1337. [CrossRef]