ORIGINAL ARTICLE

OPEN ACCESS

Impact of Cybersecurity Risks and Mitigation Strategies on Banking Industry

Hira[1], Muhammad Hafeez[2], Khadija Yasen[3], Mirza Nasir Jahan Mehdi[4]

Author's Affiliation:

Hira
BBA Scholar
Institute of Business Management Sciences, University of Agriculture Faisalabad, Pakistan.

Muhammad Hafeez
Assistant Professor
Institute of Business Management Sciences, University of Agriculture Faisalabad, Pakistan.

Khadija Yasen
Lecturer
Institute of Business Management Sciences, University of Agriculture Faisalabad, Pakistan.

Mirza Nasir Jahan Mehdi
Assistant Professor
Department of Management Sciences, Muslim Youth University Islamabad.

Article History:

Submitted: January 21, 2025
Revised: February 04, 2025
Accepted: March 24, 2025
Published online: March 28, 2025

Corresponding author(s):

Muhammad Hafeez
Muhammad.Hafeez@uaf.edu.pk

ABSTRACT

Purpose: This research focuses to evaluate the impact of cybersecurity risks impact on banks' financial performance, reputation, and customer trust, respectively. It also identifies the cybersecurity risks facing banks in this digitalized era.

Design/Method/Approach: The research uses a sample of 121 private bank users in Faisalabad, Pakistan, and apply quantitative methods, such as correlation and regression analysis, to analyze these risks and their mitigation strategies.

Findings/Results: Findings indicate that cybersecurity risks have a negative impact on banks' financial performance and reputation but drive the adoption of robust mitigation strategies. These include advanced technologies like encryption, firewalls, intrusion detection systems, and two-factor authentication, alongside employee training and regular vulnerability assessments. Despite their effectiveness, demographic and technological variations influence the degree of success, with younger, tech-savvy individuals showing greater responsiveness to mitigation efforts. Mitigation strategies have a strong positive correlation with enhanced financial performance and customer trust, thus underlining their role in building resilience.

Originality: This study shows novelty because it examines cybersecurity threats and mitigation measures in banking with emphasis on emerging threats and regional challenges. It presents findings by examining particular literature, assessing existing frameworks, and suggesting context-specific solutions addressing under-researched areas in developing economies' banking sectors.

Research Implications: The study highlights the need for collaboration between banks, fintech firms, and regulatory bodies to build integrated responses to cyber threats

Keywords: Cybersecurity Risks, Mitigation Strategies, Banking Sector; Financial Performance

JEL: D81, O31, G21, G30

1 | INTRODUCTION

The performance of the financial sector makes a country's economic development possible. It plays a vital role in industrial and agricultural growth, capital mobility, and economic stability (Tongurai and Vithessonthi 2018). Being a crucial component, the banking sector has evolved through various technological innovations. Digital change in the banking sector transforms and revolutionizes service delivery and exposes banks to certain types of risks too (Varma, Nijjer et al. 2022). In developing regions of South Asia, economic uncertainty adds towards high vulnerabilities (Essers 2013) like, financial institutions are more under stress when compared to other businesses in the region (Wong and Wei 2023). In short, stability and performance of the banking industry straight away affect the development in growth and ability of functioning as financial intermediaries for the economy. Significant indexes like profitability, productivity or efficiency, and quality assets serve to express bank success in accomplishing these objectives while sustaining confidence amongst customers (Shah and Siddiqui 2006).However, various factors, such as fraud or cyber-attacks affect their profitability and capital adequacy (Samoei and Gatobu 2024). Moreover, such threats pose risks, varying from operational failures to strategic vulnerabilities that increase the chances of bank data breaches and compliance problems (Juma'h and Alnsour 2020). Other emerging threats, especially AI-enabled attacks and susceptibility within the network of interconnected devices strain this performance further (Samoei and Gatobu 2024). Ultimately, a blow to reputation and loss of customer trust amplify this effect, reducing customer retention and acquisition and, thus undermining long-term growth and competitiveness (Hassan, Ewuga et al. 2024).

A cyber-attack refers to an activity aimed by cybercriminals to access, disrupt, and or harm the computer system, networks, or information; mainly to steal secret information, extort money, and disrupt businesses or operations (Rid and Buchanan 2015). General phrases linked to such attacks involve phishing, ransomware, distributed denial-of-service, malware, and social engineering. With growing concerns over mobile banking apps, and digital payment systems, being prime phishing and data breach targets, banks face security concerns (Gitlin and Goldstein 2015). In addition, as banks use more interconnected network devices to improve customer services, these devices open up new avenues for hackers too, increasing the possibility of data theft or service disruption (Scott 2020).

The major drivers for these emerging risks are the rapid adoption of digital technologies without a robust security framework and the sophisticated tactics of cybercriminals (Srivastava, Das et al. 2020). In addition, the evolving regulatory landscape often creates loopholes in security standards that are difficult for banks to follow.

Cybersecurity failures have long-term consequences, including loss of competitive advantage, increased operational costs for preventive measures, and erosion of customer trust (Khalil, Manzoor et al. 2021). Financial institutions that disclose robust cybersecurity measures benefit from improved market confidence and reduced investor uncertainty and on the contrary, failures damage reputation, delay partnerships, and weaken banks' resilience (Khalil 2020) .

In response, banks are investing in more advanced cybersecurity solutions, including real-time threat detection, data encryption, and multi-factor authentication (Anand, Duley et al. 2022). Furthermore, cybersecurity training for employees and cyber insurance are also being implemented to mitigate potential financial losses (Uppal 2010). However, the effectiveness of cyber insurance is still debated as it may not cover all indirect economic damages. Advanced technologies are adopted to mitigate cybersecurity risks. These technologies assist in the detection of fraud in real-time (Bhasin and Rajesh 2022). Conducting routine security audits and penetration testing is vital to identifying vulnerabilities before the cybercriminals exploit them by applying patches (Yeoh 2020). Furthermore, continued investment in training employees on increasing knowledge of emerging threats and best practices further aids in building a proactive approach (Afroz 2018). Indeed, cybersecurity remains at the top of the agenda for the banking sector as digital threats increase. By integrating robust risk mitigation strategies, enhancing transparency, and fostering collaboration, banks can safeguard customer trust, maintain financial stability, and ensure resilience against future cyber risks (Dupont 2019). The digital transformation has increased exposure of the banking industry to cybersecurity risks, which threatens operational stability, customer trust, and financial performance (Kovalenko, Sheludko et al. 2023). This research explains the cybersecurity risks in this digitalized era and the implications that banks face in such times on financial performance, reputation, and customer trust. This will be done by checking how banks mitigate such problems to reveal how such efforts may impact overall banking performance and relationships with customers.

1.1.Research Objectives

2. To identify the cybersecurity risks facing banks in this digitalized era
3. To analyze the impact of cybersecurity risks on banks' financial performance, reputation, and customer trust
4. To explore different mitigation strategies that banks implement in order to cut down their cybersecurity risks
5. To analyze the impact of banks' mitigation strategies on their financial performance, reputation, and customer trust

2 | LITERATURE REVIEW

The impact of cybersecurity risks on the banking industry is very critical since the risks that are posed by these threats significantly jeopardize the security and stability of financial institutions. Data breaches, phishing attacks, ransomware attacks, insider threats, and malware infections are all predominant in the banking industry, resulting in severe financial, operational, and reputational loss (Abrahams et al., 2024). Increased integration of technology with banking operations has made it very crucial to understand and mitigate risks for the maintenance of consumer trust, financial stability, and overall integrity of the industry (Abrahams et al., 2024). Thus, a complete review of cybersecurity risks along with the mitigation strategy is very important to secure the banking sector from any vulnerability and attack (Abrahams et al., 2024).

1. Cybersecurity Risks in Banking Industry

Cyber risks are identified as the operational threats to the informational and technological assets which have the effect on confidentiality, availability and integrity of the information (Adesuwa and David, 2019). Cybersecurity risks have become a substantial concern for financial institution due to the increasing frequency and sophistication of cyber threats. (Aljumah and Ahanger, 2020). Much scholarly research has identified key cybersecurity risks including data breaches, phishing attacks, insider threats, and malware infections (Calliess and Baumgarten, 2020).

2.1.1 Data Breaches

Data breaches present a high-risk to the Banking industries due to unauthorized access that affects the clients' sensitive information. These breaches could lead to multiple issues such as lots of financial loss, undermining reputation, and ultimately, customer’s disappointment (Carter, 2017).

Any incident of data breach can potentially cause long- term damage to a bank’s reputation, thus affecting customers and investors’ trust levels (Comizio et al., 2016)

2.1.2 Phishing Attacks

One of the most common types of cyber threats is phishing, in which banking institutions and their clients are constantly exposed to deceptive calls, emails, text messages. Phishing poses a serious risk, it is a cyber-attack where hackers impersonate legitimate organizations or individuals to trick individuals into providing sensitive information such as passwords, credit card numbers, or other personal data (Dawodu et al., 2023). Phishing is an area of major concern for the banking industry (Falch et al., 2023).

2.1.3 Insider Threats

Insider Threats remain to be unique in the banking industry since employees have authorized access to confidential systems, information and data, and they are the main area of concern from a security and

integrity point of view. Insider threats cause losses, reputational injuries, or legal repercussions for banking institutions (Haruna et al., 2022).

2.1.4 Malware Infections

The banking industry is vulnerable to malware infections, resulting in severe financial and reputational repercussions. Banking systems are infiltrated by malicious software's to steal valuable customer data, financial credentials, and sensitive business information. It is particularly challenging for financial institutions to detect and eradicate malware infections due to their treacherous nature, often leading to prolonged damage before the intrusion is even noticed (Kopp et al., 2017).

2. 2 Mitigation Strategies for Cybersecurity Risks in the Banking Industry

Implementing cyber security measures is necessary for the banking industry to secure confidential data, retain customer confidence and ensure safe financial transactions. Various cybersecurity protective methods applied by banks include firewalls, intrusion detection systems (IDS), encryption, two-factor authentication (2FA), regular vulnerability assessments, and employee awareness programs (Kshetri, 2013)

2.2.1 Firewalls

A firewall provides a vital defense by blocking unauthorized access to a bank's network and systems. Firewalls function as filters between the inside and outside networks, and they do so by examining the network traffic and implementing granular policies that are previously established to allow or deny specific data packets passing through the firewall (Peltier, 2016)

2.2.2 Intrusion Detection Systems

Intrusion Detection Systems (IDS) are an integral part of the tools having responsibility for the detection and respond to unauthorized access attempts in network bandwidth that banks are dealing with. Perwej et al., (2021) advocates the fact that IDS has multiple layers of an integrated system that can analyze data in real time to enable timely response to threat detection and potential security breaches thereby reducing the risk of data breaches.

2.2.3 Encryption

Encryption is key in data security because it enables the protection of sensitive information passing through networks, where it remains inaccessible to non-authorized persons even if it is intercepted. Solid methods of encryption allow banks to meet the demands of regulators and standards of the industry and the level of confidentiality to be heightened when executing financial operations (Sabillon, 2022).

2.2.4 Two-Factor Authentication

Two- factor authentication (2FA) is among the security features that are highly applicable in protecting banking systems by providing users with two sources of authentication before using their accounts and doing sensitive transactions. Wang et al., (2020) discover that through 2FA implementation banks add a shield that is not penetrable by hashing the users' identities being authenticated with the result of lowering the risk of credential-based attacks and unauthorized accesses (Chaudhry and Hydros, 2023)

2.2.5 Regular Vulnerability Assessments

One of the several methods of identifying and eliminating the security weaknesses in the banking systems is by conducting vulnerability assessments on a regular basis. By the vulnerability assessment processes, not only will the number of cyber-attacks be reduced but also the cybersecurity position of banks will be enhanced and strengthened (Clausmeier, 2023)

3. Impact of Cybersecurity Breaches on Banks

Cybersecurity breaches are the biggest challenges to the banking industry, and the consequences of these breaches may include financial losses, damage to reputation, legal and regulatory repercussions (Elia et al., 2023)

2.3.1 Financial Losses

The cost of cyberattacks on banks is quite high, which is inclusive of both direct and indirect expenses. Therefore, it becomes difficult to efficiently manage the issue of cyber security, especially in the financial sector. In addition, banks might be imposed regulatory fines and penalties if banks are not following data protection rules and laws or the industry rules (Hassan, et al., 2024)

2.3.2 Damage to Reputation and Customer Trust

Cybersecurity issues can damage a bank's reputation and customer trust which are both critical components in the financial industry. So, intangible costs may last for a long time. A bank's reputation for security and reliability in the financial industry is the key to success as customers evaluate their perception and brand loyalty to a bank's performance in these areas. When cybersecurity cracks occur, there is a considerable drop of customer trust in financial institutions' capability to safeguard their private information (Sabillon, 2022)

2.3.3 Legal and Regulatory Repercussions

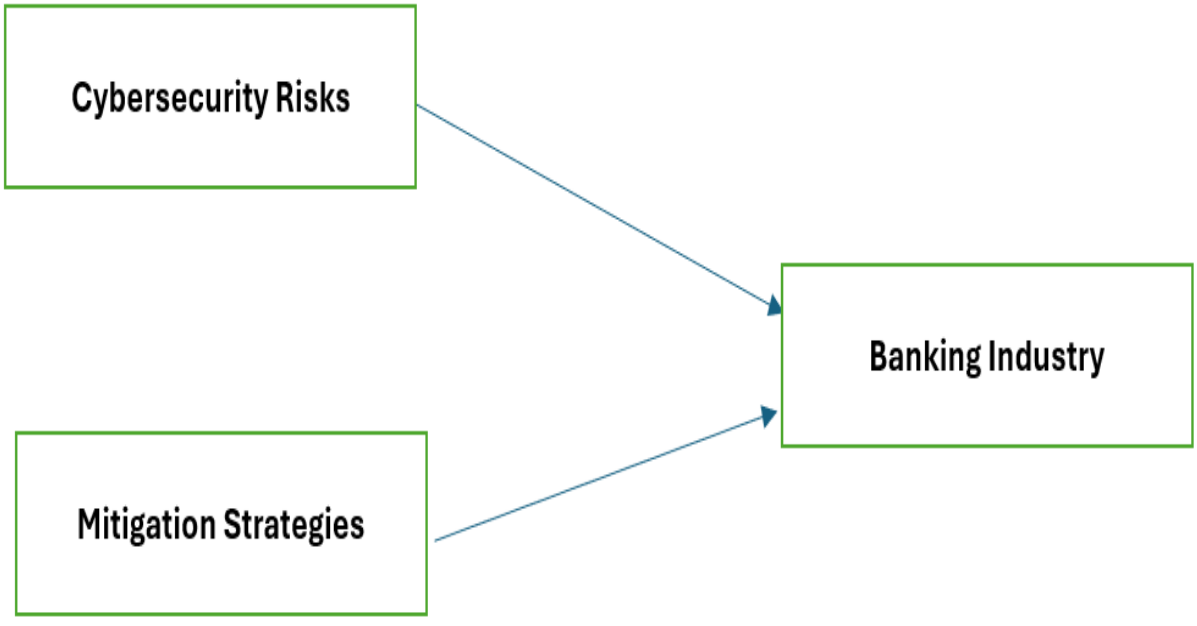
Banks are subject to legal and regulatory consequences such as fines, penalties, and the costs of litigation if cybersecurity breaches occur (Chaudhry and Hydros, 2023). Consequently, the banks will be under constant pressure from the legal and regulatory authorities, and they may face liability for the violation

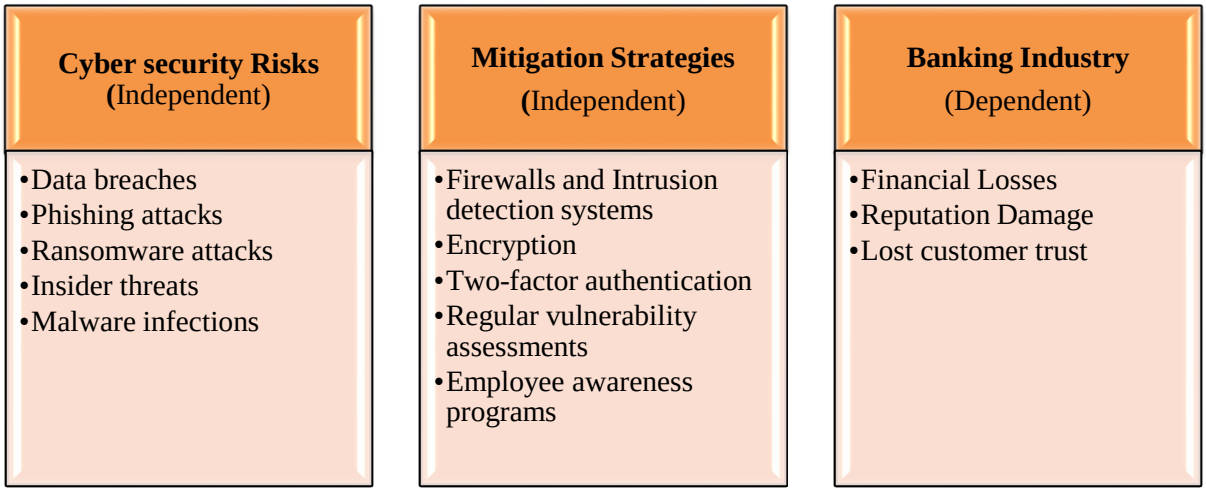
which involves fines imposed by the regulated and civil suits (Peltier, 2016). In the light of the aforementioned discussion, we have stated the following hypotheses to test private bank users of Faisalabad.

Hypothesis

1. Cybersecurity risks negatively impact financial performance, reputation, and customer trust of banks.
2. Cybersecurity mitigation measures positively impact the financial performance, reputation, and customer trust of banks

Conceptual Framework





Source: (Meland, Tokas et al. 2021), (Gavėnaitė-Sirvydienė 2024), (Amer and Al-Omar 2023),(Dawodu, Omotosho et al. 2023), (Scholtens 2000)

3 | RESEARCH METHODOLOGY AND DESIGN

This study uses a quantitative research method to understand the relationship of cybersecurity risks, mitigation techniques, and performance of the banking industry. The population for this study is composed of private bank users in Faisalabad, chosen based on their experience of using banks. The sample is taken as 121 bank users of private bank users in Faisalabad, relevant to this particular research focus. Given the limitations of resources, the sample size was found adequate to analyze associations between cybersecurity threats and the banking sector. Sample size and variables chosen can influence the reliability and validity of findings (McEwan 2020).

A self-structured questionnaire for quantitative study employs to gather data that increase the accuracy of results through statistical analysis (van Raan 2013). This approach ensures statistical analysis for reliable finding. The questionnaire was consisted of three sections: Section A of personal information, bank affiliation, and level of cybersecurity awareness. Sections B & C focused on cyber risks, incident responses, and the impact of cyber incidents on the banking industry. Respondents evaluated the effectiveness of mitigation strategies and provided insights into the effects of cyber incidents, such as financial losses, reputation damage and customer trust. To ensure the reliability, accuracy and validity of the insights gained, statistical methods are used. (Thanasegaran 2009). This research uses descriptive statistics in describing and reporting the main features of the data. For the analysis of the relationship among variables, the tool of correlation analysis is going to be used, which would determine the potential correlations among cyber risks, mitigation strategies, and performance of the banking industry. Besides, regression analysis will be used to test the strength and direction of the said relations and how the said strategies and

cyber risks affect the banks. This statistical tool allows for understanding how factors influence bank performance in this new digital era. (Sykes 1993).

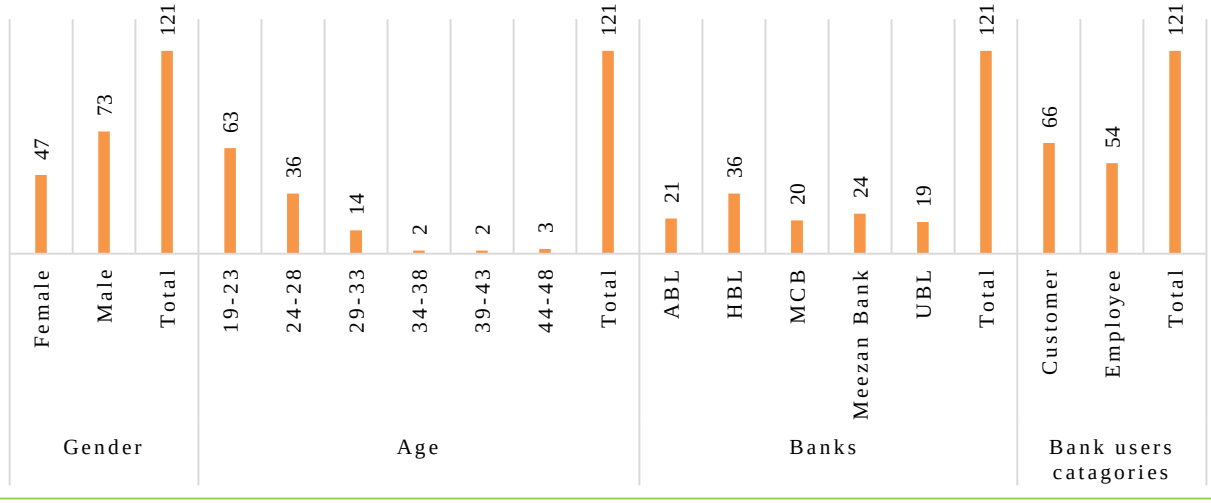
4 | ANALYSIS, RESULTS AND DISCUSSION

The **Statistical Package for Social Sciences (SPSS)** was selected as the tool for coding the data and conducting the statistical analysis. SPSS is widely used due to its ability to handle complex data and to perform a range of statistical procedures efficiently (Sun 2019). Given the relatively small sample size of **121 bank users**, SPSS was deemed the most appropriate tool to ensure accurate and reliable analysis.

In figure 1.1, the demographic distribution is a very significant part of the studies done on the banking sector as it explains consumer behavior, preferences, and decision-making processes that significantly influence services and products in the bank. (Cambra-Fierro, Perez et al. 2017). The knowledge of demographic characteristics such as gender, age, and employment status helps banks tailor their services towards different customer segments and improves the satisfaction of customers.(Kubeyinje and Osifo 2022) The data presents significant demographic insights about the sample population's gender, age, and bank affiliation. Men constitute a majority at 60.8%, while women constitute 38.8%, thereby giving a clear view of gender dynamics of bank users within the sample (36). The age distribution indicates that most of the respondents are young adults, with 52.1% falling within the age range of 19-23 years and 29.8% in the 24-28 years age group. This indicates that banking behaviors differ across age groups, with younger individuals possibly showing distinct preferences or needs in banking services (Rashid and Hassan 2009).

Demographic Distribution of Sample

Figure 1.1 Demographic Distribution



Regarding bank preferences, **HBL** emerges as the most popular, with 29.8% of respondents selecting it, followed by **Meezan Bank** (19.8%) and **ABL** (17.4%). The preferred bank distribution reflects the market

share within the surveyed segment (38). Furthermore, the sample includes both customers and employees of the banks, with **54.5%** of respondents being customers and **45.4%** employees. This distinction is crucial as bank employees and customers have differing perspectives on banking services and cybersecurity issues (Rashid and Hassan 2009). Understanding these categories enriches the analysis, ensuring a broader comprehension of stakeholder views.

4.1 Descriptive statistics

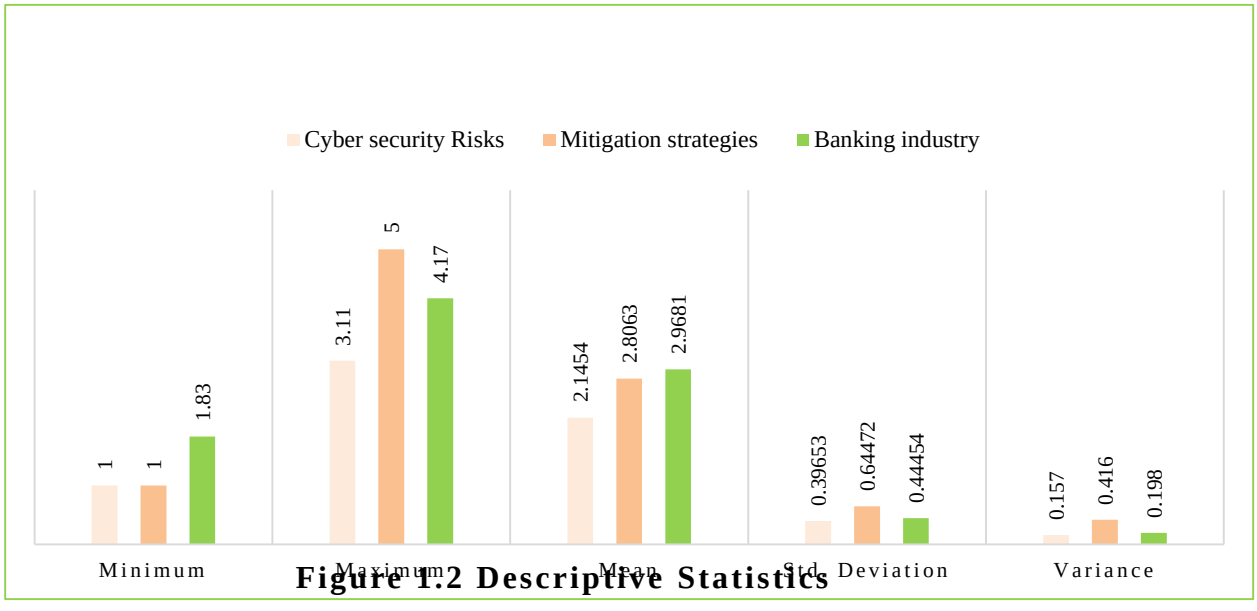


Figure 1.2 Descriptive Statistics

Descriptive statistics are vital for understanding the central tendency, variability, and range of variables in a data set (Pérez-Vicente and Ruiz 2009). Additionally, the **range** of values in the data set is shown through the minimum and maximum values, providing insight into the extent of the data's spread. The low standard deviation for Cybersecurity Risks (0.40) indicates that most responses were clustered around the average, which suggests general agreement on the level of risk. On the other hand, the higher standard deviation for Mitigation Strategies (0.64) reflects a more varied range of opinions, indicating that respondents have differing views on the effectiveness of these strategies. Variance values push the interpretations even further back; greater variance is observed with respect to Mitigation Strategies of 0.42 in comparison with Cybersecurity Risks at 0.16.

4.2 Correlation Analysis

Correlation is a statistical technique used to test the strength and direction of the relationship between two variables.(Franzese and Iuliano 2018). In banking sector studies, the correlation analysis helps identify how significant relationships are between the factors. This is beneficial in understanding how variables interact with each other in relation to cybersecurity risks and mitigation strategies. The correlation analysis shows that there are relations between Cybersecurity Risks, Mitigation Strategies, and the Banking

Industry. A strong positive correlation of 0.585 between Cybersecurity Risks and Mitigation Strategies indicates that as cybersecurity risks increase, organizations tend to adopt more mitigation strategies.(Kawimbe and Kwalombota 2024). This is in line with the trend observed globally, where higher levels of cybersecurity threats prompt the adoption of more robust security measures. (Kristian, Az-Zahra et al. 2024). However, demographic factors including age and technological proficiency would probably affect the implementation of the strategy. Younger individuals are more likely to understand these risks and push for sterner measures, whereas the older population is probably going to be less responsive and less proactive in being attentive to the changing landscape (Kshetri 2013). The negative correlation of (-0.246) for Cybersecurity Risks on the Banking Industry is indicating a moderate yet weak relationship with the fact that though the cybersecurity risks do affect the banking sector, the degree of impact is not at the expected level (Akinbowale, Klingelhöfer et al. 2020). The impacts of cybersecurity risks may vary considering the technological trends of the industry. Banks that have adopted recent technology, including AI and machine learning, are less significantly impacted by cybersecurity risks because such threats are detected better in this case (Amer and Al-Omar 2023). On the contrary, institutions with older infrastructure of technology may be inclined to feel the brunt of these risks.

Table 1.1 Correlation Analyses

		Cyber security Risks	Mitigation strategies	Banking Industry
Cyber security Risks	Pearson Correlation	1		
Mitigation strategies	Pearson Correlation	.585**	1	
Banking Industry	Pearson Correlation	-.246**	.232*	1

This indicates the secondary effect of mitigation strategies on the banking industry through a weak positive correlation at 0.232. Demographic variations also have an impact in this aspect. Young employees, more conversant with digital tools, may require aggressive mitigation measures, but older employees might be more risk-averse or less disposed to embrace new technologies (Bachaev and Karpova 2018). Technological adoption trends further complicate this relationship because banks with higher technology integration are better positioned to implement and benefit from these mitigation strategies (Alzoubi, Ghazal et al. 2022). These findings indicate that the relationship between cybersecurity risks, mitigation strategies, and the banking industry is determined by both demographic factors and technological trends. As banks continue to modernize their technological infrastructure and cater to a younger, more digitally literate workforce, the effectiveness of cybersecurity strategies will likely improve, reducing the overall impact of these risks on the sector.(Al-Sartawi, Karolak et al. 2021).

4.3 Regression Analysis

Regression analysis measures the strength and direction of relationships between predictors and predicted to have an insight into how various factors may influence a specific outcome. (Freund, Wilson et al. 2006). Regression analysis measures the strength and direction of relationships between predictors and predicted to have an insight into how various factors may influence a specific outcome. (Raghavan and Parthiban 2014). This can be attributed to the reason that high financial losses and reputational damage are brought about by cyber incidents (Anderson, Barton et al. 2019). As the strength of cyber risks becomes alarming, the costs for remediation for a breach usually make banks suffer even more hence affecting their operations and profit-making abilities (Akinbowale, Klingelhöfer et al. 2020).

Table 1.2 Regression Analyses

	Unstandardized Coefficients		**Standardized Coefficients**	**T-statistics**	**Sig.**
	B	Std. Error	Beta		
(Constant)	2.305	0.225		10.232	<.001
Cyber security Risks	-0.189	0.123	0.168	-1.534	0.028
Mitigation strategies	0.092	0.076	0.133	1.212	0.04

Conversely, **Mitigation Strategies** show a **positive relationship** (coefficient = 0.092) with the **Banking Industry**. This positive correlation aligns with previous research that suggests the effective implementation of cybersecurity measures can help protect banks from cyber threats, thereby leading to enhanced trust, customer loyalty, and financial performance. (Wang, Mao et al. 2023). The implementation of advanced security technologies, such as encryption and intrusion detection systems, often reduces the impact of cyber incidents and mitigates financial losses, that is why a positive relationship between mitigation strategies and banking industry performance is expected (Nzevela 2015).

The statistical significance of both predictors is remarkable. The significant p-values show that these relationships are unlikely to have occurred by chance and are robust enough to influence banking outcomes. (Kristian, Az-Zahra et al. 2024) emphasize the importance of understanding these relationships in the digital age, where the banking sectors must navigate growing cybersecurity threats while enhancing their mitigation strategies.

The results support the idea that while **Cybersecurity Risks** negatively affect the banking sector, **Mitigation Strategies** have a positive and significant impact, underlining the importance of proactive security

measures to protect the industry from evolving cyber threats (Nzevela 2015). As banks continue to face sophisticated threats, their investment in effective mitigation strategies can determine their ability to thrive in a digital and risk-laden environment.

Next, **model R** has a value of **0.690**, suggesting a moderately strong correlation between the observed and predicted **Banking Industry Scores** based on the two independent variables, **Mitigation Strategies Score** and **Cybersecurity Risks Score**. The value of R2 explains that about **72.4%** of the variance in the **Banking Industry Score** is explained by the two independent variables. This high R squared value shows that the model explains a significant portion of the variation, hence a good fit for the data (Freund, Wilson et al. 2006).

These statistical findings are compatible with previous studies in understanding the relationship between mitigation strategies, cybersecurity risks, and the performance of the industry. confirmed that a well-defined model, with strong predictors and minimal errors, can make good decisions for the banks. (Freund, Wilson et al. 2006) put forth the significance of making data-driven decisions in order to predict industry trends and subsequently adapting to the same by reducing risks and increasing performance.

5 | CONCLUSION

This study brings to the forefront the critical nature of securing financial systems with an increasingly common cyber threat. Data breaches, sophisticated ransomware, and phishing can have a devastating impact on banking and fintech systems, leading to financial losses and loss of customer trust that will have far-reaching damage on the stability of such institutions. The results suggest that the vulnerabilities of the cybersecurity framework can be mitigated through proactive strategies such as investment in advanced technologies, training of employees, and cross-sector collaboration. The hypothesis-01 reveals that effective implementation of cybersecurity measures can help protect banks from cyber threats, thereby leading to enhanced trust, customer loyalty, and financial performance. While it affirmed from hypothesis-02 that **Mitigation Strategies** have a positive and significant impact, underlining the importance of proactive security measures to protect the industry from evolving cyber threats

These tools enhance real-time monitoring, prevent unauthorized access, and ensure the integrity of sensitive financial data, which in turn builds more consumer confidence in digital financial services.(Al-Alawi and Al-Bassam 2020). Moreover, this study underlines the need for human-centered solutions, most of all, through training and awareness in cybersecurity. If banks can arm their employees with knowledge to help detect and reduce cyber risk vulnerabilities like phishing and malware attacks, then they may have hugely reduced internal weaknesses. (Anand, Duley et al. 2022).

The research also emphasizes that financial institutions, fintech companies, and the regulatory authorities have to cooperate with each other. Information sharing and common defense strategies will help stakeholders build a joint response to the emerging threats to foster resilience in the financial ecosystem (Bachaev and Karpova 2018). The regulatory framework has to be constantly evolving to ensure investment in cybersecurity and the alignment of the industry with the best practices for incident management and recovery. In conclusion, this research outlines the future of banking as a whole. By increasing advanced technologies, promoting cybersecurity awareness, and fostering cooperation, resilience can be enhanced to prevent cyber risks and pave for sustainable digital growth, incorporating customer trust and regulatory compliance.

5.1 RESEARCH CONTRIBUTION FOR THE FUTURE

This study recommends the use of advanced security technologies to safeguard financial transactions in the new digital world. Mass education and training programs to rectify human-centric vulnerabilities should be conducted to improve cybersecurity. Highly skilled and informed personnel reduce risks as fintech firm's work in fast-paced, digital environments.(Amer and Al-Omar 2023). The findings highlight the importance of collaboration and information sharing between fintech companies, financial institutions, and regulators in formulating joint defense strategies. Shared threat intelligence and coordinated responses strengthen cybersecurity resilience across the financial ecosystem (Afroz 2018). The study addresses all the areas mentioned above. This provides a basis for secure digital innovations, with fintech sustainable growth, capable of withstanding ever-changing cyber threats.

References

Afroz, N. N. (2018). "Effects of training on employee performance-A study on banking sector, Tangail Bangladesh." Global Journal of Economics and Business 4(1): 111-124.

Akinbowale, O. E., et al. (2020). "Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature." Journal of Financial Crime 27(3): 945-958.

Al-Alawi, A. I. and M. S. A. Al-Bassam (2020). "The significance of cybersecurity system in helping managing risk in banking and financial sector." Journal of Xidian University 14(7): 1523-1536.

Al-Sartawi, A., et al. (2021). Cybersecurity aids financial institutions performance. Big data for entrepreneurship and sustainable development, CRC Press: 91-104.

Alzoubi, H. M., et al. (2022). Cyber security threats on digital banking. 2022 1st International Conference on AI in Cybersecurity (ICAIC), IEEE.

Amer, T. B. and M. I. A. Al-Omar (2023). "The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector." International Journal of Advanced Computer Science and Applications 14(8).

Anand, K., et al. (2022). "Cybersecurity and financial stability."

Anderson, R., et al. (2019). Measuring the changing cost of cybercrime. The 18th Annual Workshop on the Economics of Information Security (WEIS 2019).

Bachaev, U. A. and T. y. A. e. Karpova (2018). "Development of the banking sector in the digital economy." Экономика: вчера, сегодня, завтра 8(9A): 20-26.

Bhasin, N. K. and A. Rajesh (2022). "The role of emerging banking technologies for risk management and mitigation to reduce non-performing assets and bank frauds in the Indian banking system." International Journal of E-Collaboration (IJeC) 18(1): 1-25.

Cambra-Fierro, J., et al. (2017). "Towards a co-creation framework in the retail banking services industry: Do demographics influence?" Journal of Retailing and Consumer Services 34: 219-228.

Dawodu, S. O., et al. (2023). "Cybersecurity risk assessment in banking: methodologies and best practices." Computer Science & IT Research Journal 4(3): 220-243.

Dupont, B. (2019). "The cyber-resilience of financial institutions: significance and applicability." Journal of cybersecurity 5(1): tyz013.

Essers, D. (2013). "Developing country vulnerability in light of the global financial crisis: Shock therapy?" Review of Development Finance 3(2): 61-83.

Franzese, M. and A. Iuliano (2018). Correlation analysis. Encyclopedia of bioinformatics and computational biology: ABC of bioinformatics, Elsevier. 1: 706-721.

Freund, R. J., et al. (2006). Regression analysis, Elsevier.

Gavėnaitė-Sirvydienė, J. (2024). "Development of cyber security assessment tool for financial institutions."

Gitlin, M. and M. J. Goldstein (2015). Cyber attack, Twenty-First Century Books.

Hassan, A. O., et al. (2024). "Cybersecurity in banking: a global perspective with a focus on Nigerian practices." Computer Science & IT Research Journal 5(1): 41-59.

Juma'h, A. H. and Y. Alnsour (2020). "The effect of data breaches on company performance." International Journal of Accounting & Information Management 28(2): 275-301.

Kawimbe, S. and M. Kwalombota (2024). "Mitigating Cybersecurity Risks in the Digitization of Banking Operations: Strategies, Challenges, and Best Practices for Zambian Commercial Banks." International Journal of Research and Innovation in Social Science 8(3s): 2988-3005.

Khalil, K. (2020). "Effect of cyber security costs on performance of e-banking in Pakistan." Journal of Managerial Sciences 14(4): 85-99.

Khalil, K., et al. (2021). "Impact of Cyber Security Cost on the Financial Performance of E-Banking: Mediating Influence of Product Innovation Performance." Humanities & Social Sciences Reviews 9(2): 691-703.

Kovalenko, V., et al. (2023). "DIGITAL TRANSFORMATION OF BANKING BUSINESS: PRESENT AND FUTURE." Socio-economic relations in the digital society 4(50): 25-40.

Kristian, A., et al. (2024). "Enhancing Cybersecurity Risk Management Strategies in Financial Institutions: A Comprehensive Analysis of Threats and Mitigation Approaches." CORISINTA 1(2): 96-103.

Kshetri, N. (2013). "Cybercrime and cyber-security issues associated with China: some economic and institutional considerations." Electronic Commerce Research 13: 41-69.

Kubeyinje, G. T. and S. J. Osifo (2022). "Demographic Differences and Customer Satisfaction towards Banking Services in Benin City, Nigeria." Journal of Entrepreneurship and Business 10(2): 106-122.

McEwan, B. (2020). "Sampling and validity." Annals of the International Communication Association 44(3): 235-247.

Meland, P. H., et al. (2021). "A systematic mapping study on cyber security indicator data." Electronics 10(9): 1092.

Nzevela, A. K. (2015). The Effect of Internet Banking Risk Management Strategies on Financial Performance of Commercial Banks in Kenya, University of Nairobi.

Pérez-Vicente, S. and M. E. Ruiz (2009). "Descriptive statistics." Allergologia et immunopathologia 37(6): 314-320.

Raghavan, A. and L. Parthiban (2014). "The effect of cybercrime on a Bank's finances." International Journal of Current Research & Academic Review 2(2): 173-178.

Rashid, M. and M. K. Hassan (2009). "Customer demographics affecting bank selection criteria, preference, and market segmentation: study on domestic Islamic banks in Bangladesh." International journal of Business and Management 4(6).

Rid, T. and B. Buchanan (2015). "Attributing cyber attacks." Journal of strategic studies 38(1-2): 4-37.

Samoei, P. C. and P. Gatobu (2024). "CYBERSECURITY AND PERFORMANCE OF INTERNET BANKING SERVICES IN COMMERCIAL BANKS IN NAIROBI CITY COUNTY, KENYA." International Journal of Social Sciences Management and Entrepreneurship (IJSSME) 8(1).

Scholtens, B. (2000). "Competition, growth, and performance in the banking industry." Center for Financial Institutions, Working Papers 00-18, Wharton School Center for Financial Institutions, University of Pennsylvania.

Scott, B. F. (2020). "Red teaming financial crime risks in the banking sector." Journal of Financial Crime 28(1): 98-111.

Shah, M. H. and F. A. Siddiqui (2006). "Organisational critical success factors in adoption of e-banking at the Woolwich bank." International Journal of information management 26(6): 442-456.

Srivastava, S. K., et al. (2020). "Determinants of cybercrime originating within a nation: a cross-country study." Journal of Global Information Technology Management 23(2): 112-137.

Sun, Z. (2019). "A study on the educational use of statistical package for the social sciences." International Journal of Frontiers in Engineering Technology 1(1): 20-29.

Sykes, A. O. (1993). "An introduction to regression analysis."

Thanasegaran, G. (2009). "Reliability and Validity Issues in Research." Integration & Dissemination 4.

Tongurai, J. and C. Vithessonthi (2018). "The impact of the banking sector on economic structure and growth." International Review of Financial Analysis 56: 193-207.

Uppal, R. (2010). "Customer complaints in banks: Nature, extent and strategies to mitigation." Journal of Economics and International Finance 2(10): 212-220.

van Raan, A. F. J. (2013). Handbook of quantitative studies of science and technology, Elsevier.

Varma, P., et al. (2022). "Thematic analysis of financial technology (Fintech) influence on the banking industry." Risks 10(10): 186.

Wang, H., et al. (2023). "Fintech inputs, non-performing loans risk reduction and bank performance improvement." International Review of Financial Analysis 90: 102849.

Wong, S. L. and M. Wei (2023). The bank vulnerability index: A health check on ASEAN+ 3 banks and banking sectors.

Yeoh, P. (2020). "Banks' vulnerabilities to money laundering activities." Journal of Money Laundering Control 23(1): 122-135.

Abrahams, T.O., Ewuga, S.K., Dawodu, S.O., Adegbite, A.O., & Hassan, A.O. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1-25. https://dx.doi.org/10.51594/csitrj.v5i1.699.

Adesuwa, E., & David, M.S. (2019). Cyber Crime and Its Economic Impact in Nigeria. South Eastern Journal of Research and Sustainable Development (Sejrsd), 2(1), 16-31.

Aljumah, A., & Ahanger, T.A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications, 14(7), 1185-1191.

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: a legal perspective. German Law Journal, https://dx.doi.org/10.1017/glj.2020.67.

Carter, W., 2017. Forces shaping the cyber threat landscape for financial institutions.

Comizio, V.G., Dayanim, B., & Bain, L., 2016. Cybersecurity as a global concern in need of global solutions: an overview of financial regulatory developments in 2015. Journal of Investment Compliance, 17(1), 101-111. 22-35. https://dx.doi.org/10.1108/JOIC-01-2016- 0003.

Dawodu, S.O., Omotosho, A., Akindote, O.J., Adegbite, A.O., & Ewuga, S.K. (2023). Cybersecurity risk assessment in banking: methodologies and best practices. Computer Science & IT Research Journal, 4(3), 220-243. https://dx.doi.org/10.51594/csitrj.v4i3.659.

Falch, M., Olesen, H., Skouby, K.E., Tadayoni, R., & Williams, I. (2023). Cybersecurity Strategies for SMEs in the Nordic Baltic Region. Journal of Cyber Security and Mobility, 11(6), 727- 754. https://dx.doi.org/10.13052/jcsm2245-1439.1161

Haruna, W., Aremu, T.A., & Modupe, Y.A. (2022). Defending against cybersecurity threats to the payments and banking system. arXiv preprint arXiv:2212.12307.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund

Kshetri, N. (2013). Cybercrime and cybersecurity in the global south. Springer.

Peltier, T.R. (2016). Information security policies, procedures, and standards: guidelines for effective information security management. CRC press.

Clausmeier, D., 2023. Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). Int. Cybersecurity Law Rev. 4 (1), 79–90.

Elia, G., Stefanelli, V., Ferilli, G.B., 2023. Investigating the role of Fintech in the banking industry: what do we know? European J. Innovation Manag. 26 (5), 1365–1393.

Hassan, A.O., Ewuga, S.K., Abdul, A.A., Abrahams, T.O., Oladeinde, M., Dawodu, S.O., 2024. Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Comput. Sci. IT Res. J. 5 (1), 41–59.