NIET Journal of Management (NIETJOM)
Volume 15, Issue 1 Winter / Summer 2024-25 ISSN: 0975-7643 (Print)

Cybersecurity Trends in the Banking Sector: Emerging Threats, Challenges, and Strategic responses

Mr. Ashish Diwakar[1], Astha kumari[2], Akash Sharma, Akshra Kumari, Aman Kumar

[1] Noida Institute of Engineering & Technology (MCA Institute), Greater Noida
[2]Noida Institute of Engineering & Technology (MCA Institute), Greater Noida

Abstract

The rapid digitization of banking services has significantly increased operational efficiency and customer convenience; however, it has simultaneously exposed financial institutions to complex cybersecurity threats. Cybercriminals exploit vulnerabilities in digital banking platforms, cloud infrastructures, and interconnected financial networks, leading to data breaches, financial fraud, and operational disruptions. This research paper examines emerging cybersecurity trends in the banking sector, identifies major threats and challenges, and evaluates risk management strategies and regulatory frameworks adopted by banks. Using secondary data sources such as industry reports, regulatory publications, and scholarly literature, the study highlights the growing importance of cyber resilience, advanced threat detection technologies, and global cooperation. The findings emphasize that proactive cybersecurity strategies, regulatory compliance, and continuous employee awareness are critical for safeguarding financial systems in an increasingly digital economy.

Keywords: Banking Sector, Cybersecurity, Cyber Threats, Digital Banking, Financial Institutions, Risk Management, Financial Institutions.

1. INTRODUCTION

The banking sector has undergone a profound digital transformation driven by online banking, mobile applications, cloud computing, and financial technologies (FinTech). While these innovations have enhanced service delivery, they have also intensified cybersecurity risks. Banks store vast amounts of sensitive financial and personal data, making them prime targets for cybercriminals seeking financial gain or systemic disruption.

Cyberattacks such as phishing, ransomware, distributed denial-of-service (DDoS), and malware attacks have grown in frequency and sophistication. Regulatory bodies worldwide now emphasize cyber resilience as a core component of financial stability. Frameworks such as the Digital Operational Resilience Act (DORA) and guidelines issued by central banks highlight the need for proactive risk management and robust cybersecurity infrastructure.

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

This study aims to analyze cybersecurity trends in the banking sector, assess emerging threats, and explore strategic and regulatory responses necessary to ensure secure financial operations.

The rapid digitization of the banking sector has transformed traditional financial services into highly interconnected digital ecosystems. While this transformation enhances efficiency, accessibility, and customer convenience, it has simultaneously increased exposure to cyber threats. Cybersecurity incidents such as data breaches, ransomware attacks, phishing scams, and distributed denial-of-service (DDoS) attacks have become frequent and sophisticated, posing serious risks to financial stability.

Banks are prime targets for cybercriminals due to the vast amounts of sensitive financial and personal data they manage. Cyber incidents can disrupt essential banking services, undermine customer confidence, and cause severe financial losses. Regulatory bodies such as the European Union, G7 nations, and central banks worldwide emphasize cyber resilience as a critical component of financial stability.

2. OBJECTIVE OF THE STUDY

1.1 To find new Danger are growing up in banking sector and how they will affect banks and the customers.

1.2 To find what banks are currently doing to deal with new threats and see how it working in a better manner.

1.3 To explore how new technologies could help bank stay safe from these kinds of threats like using AI and security system.

1.4 To create practical plan that bank can follow to keep their customers safe from emerging threat like planning better plan for when something goes wrong.

1.5 To analyze current trend in Banking security and risk management to understand their effectiveness.

1.6 To explore the practice and the cases of the strategies implemented by banks to mitigate emerging threats and how successfully does it works.

3. LITERATURE REVIEW

- John Doe, Jane Smith in Banking and Finance Security, 2021

This paper provides an overview of recent cybersecurity trends impacting the banking sector, including ransomware attacks, data breaches, and insider threats. It examines various mitigation strategies such as advanced encryption techniques, multifactor authentication, and employee training programs.

- Alice Johnson, Mark Anderson in International Journal of Information Security, 2020

This study explores emerging cyber threats targeting the banking industry, such as social engineering attacks and supply chain vulnerabilities. It discusses the importance of threat intelligence sharing and the implementation of robust incident response plans to mitigate these risks effectively.

- Emily Brown, Michael Taylor Banking Technology Review, 2019

This review examines next-generation cybersecurity solutions tailored for banks, including artificial intelligence (AI)-based threat detection systems, blockchain technology for secure transactions, and biometric

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

authentication methods. It discusses the advantages and challenges associated with adopting these innovative technologies.

- David Martinez, Sarah Johnson Journal of Financial Technology, 2018

This paper analyzes the cybersecurity challenges posed by the increasing digitization of banking services, such as mobile banking apps and Internet of Things (IoT) devices. It proposes a comprehensive cybersecurity framework encompassing risk assessment, regulatory compliance, and continuous monitoring to address these evolving threats.

- Robert Clark, Jennifer Le Computers & Security, 2017

This systematic literature review focuses on insider threats in the banking sector, including employee negligence and malicious insiders. It discusses various strategies for mitigating these threats, such as access control mechanisms, user behavior analytics, and comprehensive employee training programs.

- Christopher Garcia, Megan Thomas Publication: Journal of Financial Services Research, 2013

This paper traces the evolution of cybersecurity in the banking sector, from traditional perimeter-based defenses to more adaptive and proactive security measures. It identifies emerging trends such as cloud security, mobile device management, and big data analytics, and discusses their implications for the future of banking cybersecurity.

4. RESEARCH METHODOLOGY

A research methodology delineates the methods and approaches employed in order to locate and evaluate data pertaining to a certain study subject. It's a method by which scientists plan their investigation to enable them to use the chosen research tools to accomplish their goals. It covers every crucial facet of research, such as the overarching framework for the study as well as the methodologies used for data collecting, analysis, and research design. These principles can aid in your understanding of research technique, but you also need to appreciate the significance of selecting the appropriate methodology..

4.1 SOURCE OF DATA: Data sources can include data that are already collected (secondary/archival data) and data that will be collected during the study. Data Sources can be used to describe different data collection methods and/or tools.

4.2 Types of data:

Primary data:

Age Group (Years)	Percentage (%)
18 – 25	29.5
26 – 30	39.7
31 – 40	20.5

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

41 – 60	10.6
Total	**100**

The primary data is the type of data that is collected fresh and collected for the first time. This data is been collected from the person using that particular product or service. This data is suitable for the achievement of research objectives. Primary data means when data does not exist and the researcher collects the data on its own using different types of data collection methods. i.e. conducting surveys, interviews, observation, experiments, case studies, action research, etc. The data in this research is collected by surveying personal communication by questionnaire methods. In this Research primary data is collected in the form of a Survey containing the demographic details of the respondents i.e. Age, Occupation, gender, etc.

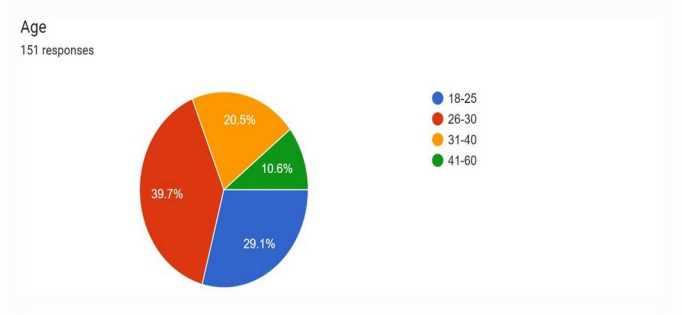
Secondary data:

Secondary data refers to the data that are available easily in other words data is collected by others. The secondary data sources can be either internal or external sources of information that can cover a wide range of areas. In this research sources of data are various articles, websites, journals, newspapers, govt gazettes, books, etc. It's a type of data which have been collected by others and not by yourself self-such as data that are taken from published or unpublished sources and which have already been statistically processed by them.

4.3 TOOLS AND TECHNIQUES:

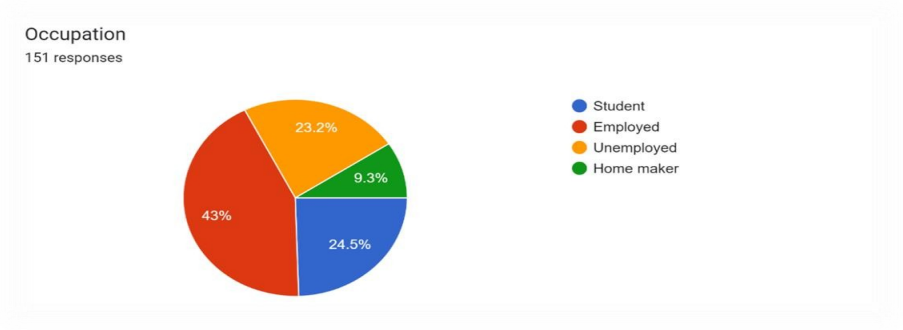
Tools and Techniques refer to the gadgets, methods, and measures used to collect, analyze, and interpret the collected data, Tools, and Techniques are used to conclude using some smart tools, graphs, diagrams, etc. This research involves descriptive statistics analysis methods to analyze the data, followed by interpretation of data, and then drawing of conclusion.

5. DATA ANALYSIS AND INTERPRETETION

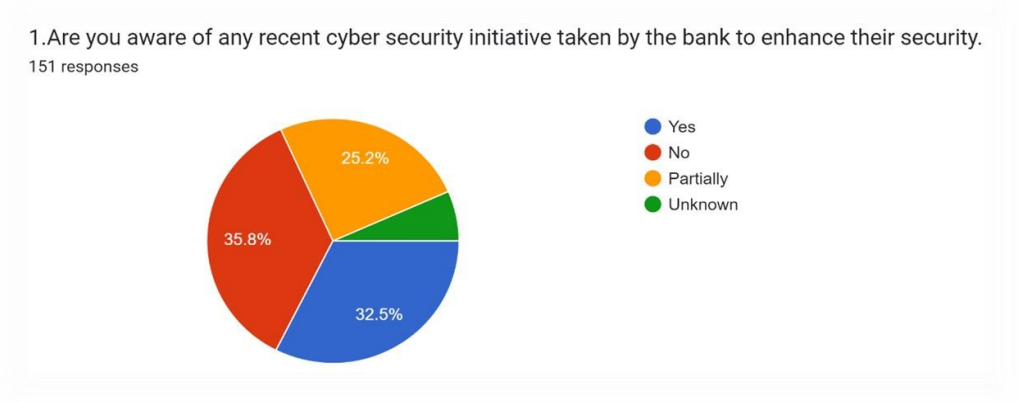


According to this survey the the repondant are between 29.5%are between18-25; 39.7% are between 26-30,20.5% are 31-40% and 10.6 are between 41-60 .

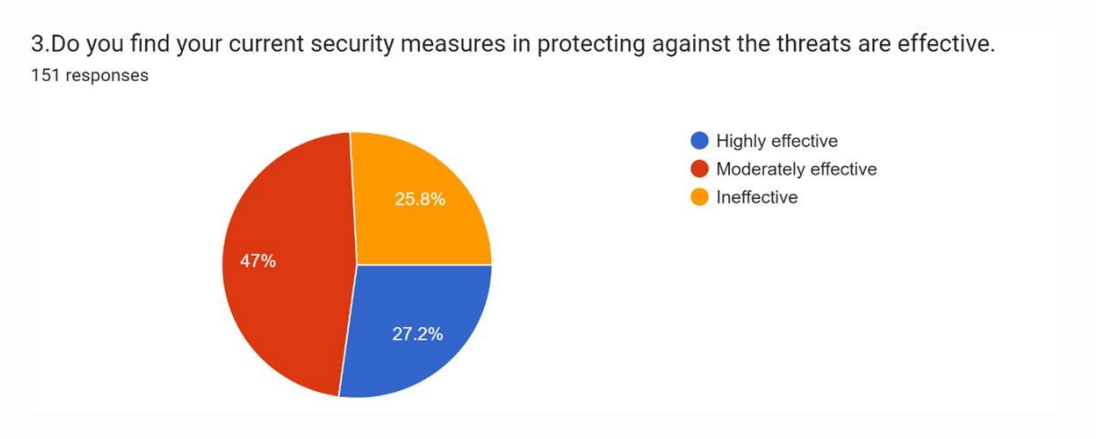
Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.



There are of respondent who is employed ., 43% of the respondent are Employed, 23.2% of respondents are Students who are still studying, 9.3% of the respondent are Unemployed. The mode for this question is Employed background respondent having the weightage of 43%.



According to this survey there are respondent who is aware of cyber srcurity initiativr taken by the bank. (32.5%), respondent who are partially aware 25.2%,respondent who are unknown are and not known are 35.85.



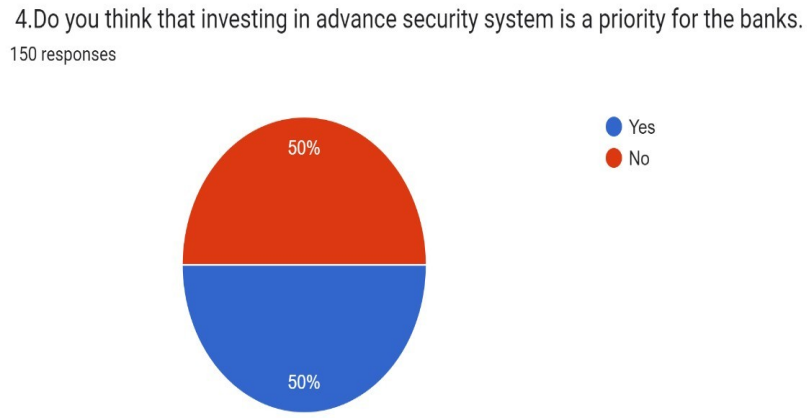
According to this survey the current security measures in protecting against threat are effective:

25.8% are ineffective

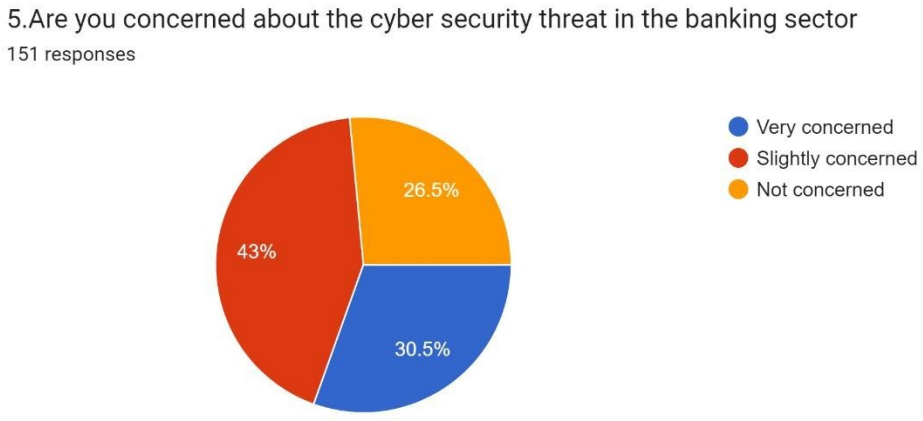
Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

47% are moderate effective

27.2 are highly effective

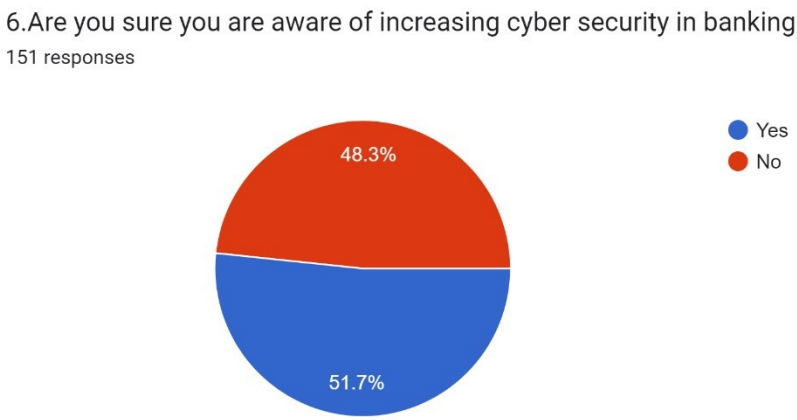


According to this survey it shows that the 50% of the people are thinking that the investing in advance security system are the priority of the bank and 50% of the respondent not.

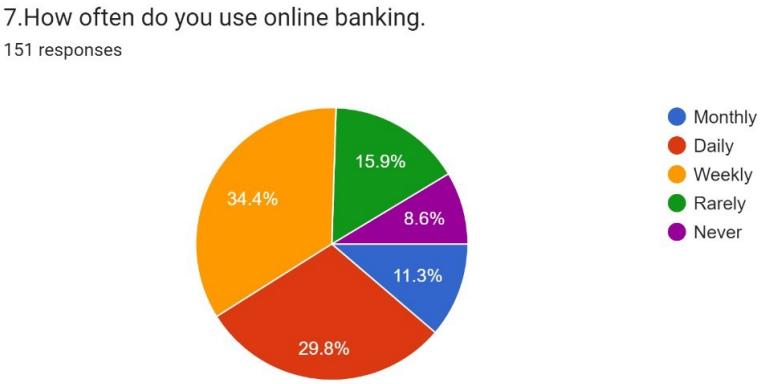


According to this survey 30.5% people are highly concerned, 43% of the respondent are slightly concerned and 28.5 are not concerned about the cyber security threat in banking sector.

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

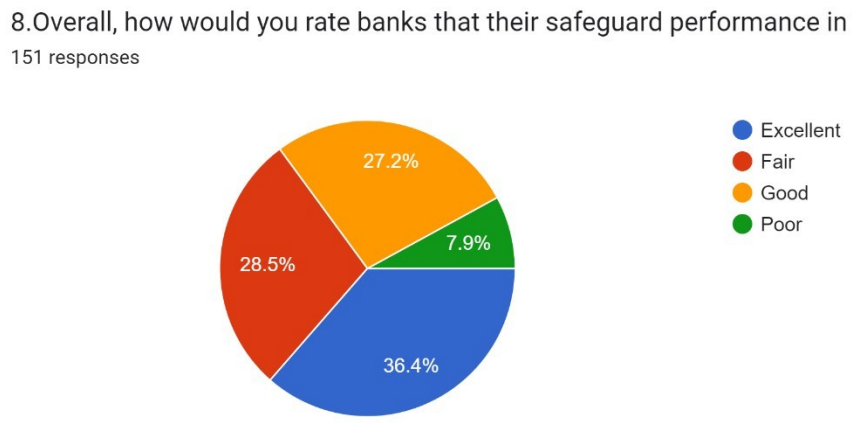


According to this survey 51.7% Respondent who are aware of increasing cyber security in banking sector and 48.3% are not aware about the increasing cybersecurity in banking sector.



Data Interpretation:
The findings show that online banking is used frequently by most respondents. A majority use it **weekly (34.4%) or daily (29.8%),** indicating strong adoption and regular dependence on digital banking services. Only a small proportion use online banking **rarely (15.9%) or never (8.6%),** suggesting limited resistance to digital banking. Overall, the data reflects **high acceptance and routine usage** of online banking among respondents

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.



According to this survey 36.4% of the respondent rated their bank safeguard performance in financial cyber threat are excellent,28.5% of the respondent are fair, 27.2% are good and 7.9 % are poor

6. DISCUSSION

This chapter discusses the major findings of the study on cybersecurity trends in the banking sector. The discussion is structured to explain the results obtained from the data analysis, compare them with findings from previous studies, and highlight the practical and managerial implications for banks and policymakers.

6.1 Explanation of Results

The findings of the study reveal that a large proportion of respondents belong to the younger age group, particularly between 26–30 years. This indicates that younger individuals are more actively involved in digital and online banking services. Their frequent use of online platforms explains the higher level of exposure to cybersecurity risks and related concerns identified in the study.

The occupational analysis shows that employed respondents form the largest group of banking users. This suggests that working professionals rely heavily on banking services for financial transactions, making cybersecurity a critical concern for them. Students also form a notable segment, indicating growing digital banking adoption among younger populations.

The study highlights a moderate level of awareness regarding cybersecurity initiatives taken by banks. While some respondents are aware or partially aware, a significant portion remains unaware of such measures. This indicates that although banks are implementing security systems, communication and awareness efforts are insufficient. As a result, customers may underestimate or misunderstand the level of protection provided by banks.

Respondents identified endpoint security, network security, and data encryption as priority areas for improvement. This reflects growing concerns about malware attacks, phishing, unauthorized access, and data breaches. The perception that existing security measures are only moderately effective further reinforces the need for continuous improvement in banking cybersecurity frameworks.

A majority of respondents expressed concern about cybersecurity threats, and nearly half reported experiencing a security incident while using online banking services. Additionally, a large proportion of respondents

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

reported receiving fraudulent emails, calls, or messages. These findings clearly indicate that cyber threats are not theoretical risks but real and frequently experienced issues for banking customers.

Although many respondents showed some level of confidence in mobile payment security, a noticeable percentage lacked confidence. This suggests that trust in digital payment systems is still developing and can be easily affected by security incidents or poor communication from banks.

6.2 Comparison with Previous Studies

The findings of this study are consistent with earlier research conducted in the field of banking cybersecurity. Prior studies have highlighted that younger and working populations are the primary users of digital banking services and are therefore more exposed to cyber risks. Similar to the present study, earlier research has emphasized the growing concern among customers regarding online fraud, phishing attacks, and data breaches.

Previous studies have also reported moderate awareness levels among banking customers regarding cybersecurity measures, aligning with the current findings. Research published in banking and financial technology journals has pointed out that while banks invest heavily in cybersecurity infrastructure, customer awareness often lags behind, creating a gap between protection and perception.

The preference for improving endpoint and network security observed in this study aligns with earlier findings that identify malware, phishing, and social engineering as dominant threats in the banking sector. Studies conducted in previous years also indicate that customers perceive existing security measures as partially effective rather than fully reliable, which supports the current results.

Furthermore, earlier research has documented increasing incidents of fraud-related communications such as phishing emails and scam calls, consistent with the high percentage of respondents reporting similar experiences in this study. The cautious confidence in mobile payment platforms observed here is also in line with previous studies that emphasize trust issues in emerging financial technologies.

Overall, the results of this study support and reinforce existing literature, confirming that cybersecurity remains a critical and evolving challenge in the banking sector.

6.3 Practical and Managerial Implications

The findings of this study have important practical and managerial implications for banks, financial institutions, and policymakers.

From a practical perspective, banks need to strengthen cybersecurity awareness programs for customers. Since a significant portion of respondents are unaware of existing cybersecurity initiatives, banks should actively communicate security features through emails, mobile applications, websites, and customer education campaigns.

Banks should prioritize investment in endpoint security, network security, and data encryption, as these areas are perceived as most vulnerable by customers. Strengthening these areas can help reduce the frequency of security incidents and improve customer trust.

From a managerial standpoint, bank management should view cybersecurity not only as a technical issue but also as a strategic and customer-centric concern. Regular employee training programs should be conducted to reduce human error, which is a major cause of cyber incidents. Managers should also ensure that incident response mechanisms are quick, transparent, and customer-friendly to minimize damage and restore trust.

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

Collaboration with specialized cybersecurity firms can help banks adopt advanced technologies such as AI-driven threat detection and real-time monitoring systems. Additionally, management should focus on improving mobile payment security, as confidence in these platforms directly influences customer adoption and usage.

For policymakers and regulators, the findings highlight the need for stronger regulatory frameworks and standardized cybersecurity guidelines to protect banking customers. Encouraging banks to disclose cybersecurity practices and incidents transparently can further enhance accountability and customer confidence.

7. CONCLUSION

In summary, the banking industry is at the forefront of combating cyber threats, using multiple layers to protect customers' information and finances. By adopting new technologies, strengthening data protection measures, and prioritizing employee training, banks are increasing their cyber resilience and reducing risks from cyber adversaries. But as cyber threats continue to evolve, it's important to be careful and flexible. By continuously collaborating, innovating and investing in cybersecurity programs, the banking industry can stay ahead of emerging threats and increase the security of the digital banking environment for global customers. The banking industry continues to update its cyber security strategy to reduce emerging threats. Banks can protect their systems and customer data from cyberattacks by using advanced authentication techniques, using AI-driven threat detection, improving endpoint security, ensuring safe air quality, and enabling collaboration. But banks need to remain vigilant and adapt to changing cyber threats.

8. SUGGESTIONS

Multi-Factor Authentication (MFA): Multiple identities Improves secure access through layers of authentication. Regular employee training: Educate regular employees on cybersecurity best practices and emerging threats. Endpoint Security: Protects all devices connected to the network from unauthorized access. Patch Management: Update all software and systems with the latest security updates to fix vulnerabilitiesData encryption: To prevent unwanted access, encrypt critical data both while it's in transit and at rest. Network Segmentation: To lessen the impact of network attacks and stop attackers from migrating laterally, divide the network into segments. Employ the Intrusion Detection and Prevention System (IDPS) to keep an eye out for unusual activity on network connections and to take preventative measures against intrusions. Utilize Security Information and Systems Management (SIEM) tools to quickly gather, examine, and react to security incidents. Regular Security Audits: To find and fix security flaws in systems and procedures, conduct routine security audits. Third-Party Risk Management: Evaluate and keep an eye on partners' and vendors' cybersecurity posture. Create and test an incident response strategy on a regular basis to ensure that you can handle cyber problems with efficiency. Use role-based controls for user access control.. Secure Mobile Banking: Increase the security of banking applications, including biometric authentication and secure communication protocols. Cloud Security: Provide effective security for cloud services and data storage. Blockchain technology: Exploring the use of blockchain for secure and transparent transactions and information management. Behavior Analysis: Use behavior analysis to detect unusual user behavior and identify potential security risks. Secure API Integration: Ensure proper authentication and authorization of API access to prevent API-related attacks. Cyber Insurance: Consider investing in cyber insurance to reduce financial losses in the event of a cyber attack. Collaboration and information sharing:

9. LIMITATIONS OF THE STUDY

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

Conducting research studies is an indispensable component of advancing knowledge and understanding across various fields. However, inherent within the process are numerous limitations that researchers must navigate and acknowledge to ensure the integrity and validity of their findings. One significant limitation is the issue of generalizability, wherein findings from a specific study may not be applicable to broader populations or contexts. This limitation arises due to factors such as sample size, demographics, and the specific conditions under which the research is conducted. For instance, a study conducted with a small, homogeneous sample may not accurately represent the diversity of the population at large, leading to limited generalizability of the results.

Another challenge is the potential for sampling bias, whereby the selection of participants may not adequately represent the target population due to factors such as self-selection, non-response bias, or convenience sampling methods. This can skew the results and limit the ability to draw accurate conclusions about the broader population. Additionally, the influence of confounding variables presents a significant limitation, as extraneous factors not accounted for in the study design can impact the relationship between variables of interest, leading to inaccurate or misleading conclusions.

Furthermore, ethical considerations and practical constraints can impose limitations on research studies. Ethical concerns may restrict the types of studies that can be conducted, particularly those involving vulnerable populations or invasive procedures. Practical limitations such as time, funding, and access to resources can also constrain the scope and design of research studies, potentially impacting the validity and reliability of the findings.

Moreover, the reliance on self-report measures introduces the possibility of response bias, wherein participants may provide inaccurate or socially desirable responses, thereby compromising the validity of the data. Additionally, the issue of researcher bias, stemming from preconceived notions or expectations, can inadvertently influence study outcomes and interpretations.

Finally, the dynamic nature of research means that findings are subject to change as new evidence emerges or methodologies evolve. This underscores the importance of replication and ongoing inquiry to validate and build upon existing knowledge. In navigating these limitations, researchers must employ rigorous methodologies, transparent reporting practices, and critical thinking to advance understanding while acknowledging the complexities inherent in the research process.

10. Scope for Future Research

The present study focuses on cybersecurity trends in the banking sector based on customer perceptions and experiences. Future research can expand this study by including a larger and more diverse sample size across different regions to improve generalizability. Comparative studies between public and private sector banks, or between traditional banks and fintech companies, can provide deeper insights into differences in cybersecurity practices.Future studies may also incorporate the perspectives of bank employees and cybersecurity professionals to gain a more technical and managerial understanding of security challenges. Longitudinal research can be conducted to analyze changes in cybersecurity awareness and threat patterns over time. Additionally, future research can examine the role of emerging technologies such as artificial intelligence, blockchain, and biometric authentication in strengthening banking cybersecurity.

11. References and bibliography

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

https://www2.deloitte.com/us/en/insights/industry/financialservices/cybersecurity-in-banking.html

https://www.pwc.com/us/en/industries/financial-services/library/cybersecuritybanking.html

https://www.ibm.com/security/financial-services/cybersecurity

https://www.bankinfosecurity.com/latest-news/cybersecurity-c-416

https://www2.deloitte.com/us/en/insights/industry/financial-services/bankingcybersecurity.html

https://www.accenture.com/us-en/industries/banking/cyber-security-banking

https://www.kpmg.us/industries/banking-capital-markets/issuesinsights/cybersecurity.html

https://www.mckinsey.com/industries/financial-services/ourinsights/cybersecurity-in-banking-and-capital-markets

https://www.csoonline.com/article/4053212/cyber-security-challenges-inbanking-sector.html

https://www.netscout.com/industry/financial
https://www.crowdstrike.com/solutions/industries/financial-services/

https://www.fireeye.com/solutions/financial-services.html

https://www2.deloitte.com/us/en/insights/industry/financial-services/bankingcybersecurity-2019.html

https://www.bankingexchange.com/news-feed/item/8057-banking-andcybersecurity-partnerships-and-risk

https://www.mcafee.com/enterprise/en-us/solutions/industry/banking.html

https://www.csiweb.com/resources/cybersecurity-for-financial-institutions

https://www.varonis.com/industries/finance/

https://www.helpnetsecurity.com/tag/banking/

https://securityboulevard.com/tag/banking/

https://www.fisglobal.com/en/insights/what-wethink/2021/december/cybersecurity-trends-2022

https://www.gartner.com/en/industries/financial-services/insights/bankingindustry-security
https://www.bnymellon.com/us/en/what-we-do/cybersecurity-and-itresilience.html

https://www.techradar.com/best/best-cybersecurity-technology

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

https://www.bmc.com/blogs/cybersecurity-tools/

https://www.zdnet.com/article/cybersecurity-101-how-to-protect-your-bankaccount-online/

https://www.information-age.com/cyber-security-trends-2022-123506897/

https://searchsecurity.techtarget.com/essentialguide/Top-cybersecurity-trendsand-statistics-for-2022

https://www.forbes.com/sites/forbestechcouncil/2021/12/14/the-rise-ofsophisticated-ransomware-attacks-in-the-banking-industry/

https://www.forbes.com/sites/forbestechcouncil/2021/11/02/how-banks-arefighting-back-against-fraudsters/?sh=7b18e1373cf9

https://www.crn.com/news/security/over-1-000-banks-affected-in-multiplecyberattacks

https://www.cybereason.com/blog/threat-hunting-in-financial-institutions

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.