Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
March 2025 13(3), 568–574

CYBERSECURITY RISKS AND MITIGATION STRATEGIES IN THE INDIAN BANKING SECTOR

Namrata Verma [1], Dr. Sanyam [2]

[1] Associate Professor Psychology, Rajkiya Mahavidyalay Modinagar, Ghaziabad, India
[2] Assistant Professor Cpommerce Rajkiya Mahila Mahavidyalaya Nagla Kashi, Dhaulana, Hapur

Received 07 December 2024
Accepted 08 January 2025
Published 31 March 2025

Corresponding Author

Namrata Verma,
Namrata9476@gmail.com

DOI
10.29121/granthaalayah.v13.i3.2025.6870

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The rapid-fire digitalization of fiscal services has significantly impacted the global fiscal assiduity, particularly the banking assiduity, with significant changes observed in the fiscal systems of arising husbandry similar as India. Digital banking, mobile payment systems, and online fiscal services have bettered the fiscal assiduity's effectiveness and fiscal addition. still, the increased use of digital structure has also redounded in exposure to a wide range of cyber security pitfalls. Cyber security pitfalls similar as phishing, ransomware, malware, bigwig attacks, and data breaches pose significant pitfalls to the fiscal assiduity and its guests. The fiscal assiduity of India has come a seductive target for cybercriminals because of the increased digitalization of fiscal systems and the high volume of fiscal deals reused on a diurnal base. This study aims to identify the primary cyber security pitfalls faced by the fiscal assiduity of India and assess the effectiveness of the cyber security mitigation strategies espoused by fiscal institutions. The qualitative system has been used to conduct the study, and secondary data has been used, which has been attained from the literature review of colourful publications, reports, and papers. The results attained indicate that cyber pitfalls in the fiscal assiduity are rising with the increase in technology, cyberattack methodologies, and the lack of cyber security mindfulness among the general public. The results also indicate the part of technology, similar as artificial intelligence, blockchain technology, and biometric technology, in perfecting the cyber security of the fiscal assiduity. Eventually, the results attained in the study are presented with suggestions and recommendations for the development of an effective cyber security strategy, which can be used to alleviate cyber security pitfalls and ensure the development of robust cyber security systems to insure the trustability and responsibility of the digital fiscal ecosystem of India.

Keywords: Banking, Data Breach, Fiscal Ecosystem, OTP and MFA

1. INTRODUCTION

The managing an account division plays a essential portion in supporting productive development and monetary steadiness. In later times, innovative development has essentially changed over the operations of keeping money educate. The development of computerized managing an account administration, counting web keeping money, versatile keeping money, and genuine- time instalment frameworks, has upgraded accessibility, comfort, and adequacy for

visitors. India has persevered rapid-fire development in computerized financial administrations over the once decade. Government venture pointed at advancing advanced instalments and financial expansion have quickened the relinquishment of electronic keeping money stages. The including infiltration of smartphones, tall-speed web network, and monetary innovation comes about has assist contributed to the development of computerized managing an account administration. In spite of the multitudinous benefits of advanced transformation, the developing dependence on advanced innovations has made unused vulnerabilities in keeping money frameworks. financial educate store and prepare huge volumes of touchy data, counting client individualities, financial records, and deal information. In like manner, the keeping money division has come a essential target for cybercriminals looking for monetary pick up or key disengagement.

Cybersecurity pitfalls have come decreasingly advanced and fragile to descry. Cyberattacks comparative as phishing cheats, malware diseases, ransomware assaults, and information breaches can conceive critical monetary misfortunes and harm the character of monetary teach. too, cyber episodes may disturb keeping money operations and weaken open certainty in computerized monetary administrations. The including complexity of cyber pitfalls highlights the require for vigorous cybersecurity textures inside the managing an account segment. Viable cybersecurity techniques bear a combination of mechanical comes about, nonsupervisory oversight, danger operation hones, and cybersecurity mindfulness among specialists and visitors.

This think about points to look at the cybersecurity pitfalls confronted by the Indian managing an account division and gauge relief procedures that can improve cyber flexibility. By assaying being investigation and assiduity reports, the paper gives perceptivity into the advancing cybersecurity topography and distinguishes certain comes about for reinforcing keeping money security.

2. PROBLEM STATEMENT

The fast extension of computerized keeping money administrations in India has altogether expanded the introduction of money related educate to cyber dangers. Whereas banks have received different mechanical arrangements to move forward operational proficiency, numerous teach still confront challenges in actualizing comprehensive cybersecurity frameworks.

Cyberattacks focusing on keeping money frameworks have gotten to be more visit and advanced, posturing genuine dangers to money related soundness, client security, and regulation notoriety.

Despite executive trials and innovative marches, multitudinous banks do to battle with cybersecurity vulnerabilities. Subsequently, there is a require to methodicallly look at the cybersecurity dangers influencing the Indian managing an account division and assess compelling relief strategies.

3. LITERATURE REVIEW

3.1. CYBERSECURITY IN MONETARY SYSTEMS

Cybersecurity alludes to the assurance of computer frameworks, systems, and advanced data from cyber dangers and unauthorized get to. Agreeing to Anderson et al. (2019), cybercrime has gotten to be one of the most noteworthy dangers confronting advanced budgetary frameworks. The expanding reliance on computerized framework has extended the assault surface for cybercriminals.

Financial educate are especially helpless to cyberattacks since they oversee important budgetary resources and touchy information.

3.2. COMPUTERIZED MANAGING AN ACCOUNT AND CYBER RISK

The computerized change of money related administrations has presented various mechanical advancements in the keeping money segment. Arner et al. (2017) contend that fintech advancements have altogether progressed popular consideration and functional proficiency. In addition, these advances have also posed a number of cybersecurity challenges.

The integration of protean keeping plutocrat operations, pall computing stages, and third- party plutocrat related administrations has expanded the complexity of keeping plutocrat fabrics and extended implicit section focuses for cyberattacks.

3.3. COMMON CYBER RISKS IN BANKING

Research thinks about recognize a few major cyber dangers influencing the keeping money segment. Phishing assaults are among the most common troubles, as cybercriminals use deceiving communication strategies to get secret data from guests Hadnagy (2018).

Malware assaults and ransomware occurrences are moreover predominant dangers that can compromise managing an account framework and disturb money related operations. Agreeing to Romanosky (2016), ransomware assaults have expanded essentially in later a long time, especially in businesses taking care of delicate budgetary information.

Table-1

Table 1 Major cybersecurity Threats in Banking Sector in India

Cyber Threatt	Description of Cyber Threat	Impact on Banking System
Phishing	Fraudulent E-Mail or messages are used to steal login credentials	Unauthorised account access
Malware	Malicious software is installed that infiltrates the banking system	System is compromised and data theft
Ransomware	Data is encrypted and ransom demand	Operational disruption
Data Vulnerability	weakness in system, software or human processes	unauthorised access to sensitive information of individual or corporate
Insider Threat	Authorised access is misused by employees	Data leaks and financial frauds
Sim Swapping	Mobile number is fraudulently transferred to attackers	OTP interception and account is takeover by attackers

4. RESEARCH METHODOLOGY

4.1. RESEARCH DESIGN

The study is based on qualitative research design so as to analyse the cybersecurity risk and mitigation strategies in the banking sector of India. The qualitative approach allows an in-depth examination of cybersecurity challenges and solutions on the bases of existing literature and industry data.

4.2. DATA COLLECTION

The secondary data was used in the study which collected from-

- Academic Journals accompanying cybersecurity, FinTech and Digital Banking System
- Government reports on banking
- Industrial publication

4.3. OBJECTIVES OF STUDY

- To Identify and analyse major types of cyber risks faced by banks
- To suggest suitable strategies and best practices for strengthening cyber risk management

5. RISK OF CYBER SECURITY IN INDIAN BANKING SYSTEM

5.1. PHISHING AND SOCIAL ENGINEERING

It is an attempt to pilfer sensitive information of customer by pretending to be trustworthy. The customer might get an E-Mail that looks like it is from the bank or customer may get a text message saying his delivery needs confirmation. it looks like normal but behind it is a fraudster. Without social engineering phishing is not possible to be succeed its helps to understand how individuals respond under pressure. Psychology is more often used by attackers than technology.

Phishing isn't just one method instead takes many forms-

- E-Mails containing fake links
- Text messages containing links to harmful websites
- Phone calls in which the caller claims to be an official
- Social media chats asking for personal information

Preventions strategies from phishing attacks

- Anti-phishing plug-ins can be used that warn before clicking a harmful link
- E-Mail gateways can be used so as to filter suspicious content
- Training Programs can be organised that simulate phishing attacks to prepare employees

5.2. MALWARE AND BANKING TROJANS

Malware is malicious software that is designed to disrupt, damage or steal sensitive information from user's device. Banking trojans is also a malware that is specially designed to target online banking platforms and capture login credentials, debit card/credit card information One Time Passwords (OTP) and Multi Factor Authentication (MFA) codes, session data and device fingerprints etc. Banking trojans target those users and organisations that regularly access financial services online. The common banking trojans are- Zeus(Zbot), TrickBot, Emotet, Dridex and Mobile banking trojans.

Preventions Strategies from Malware and banking trojans-

An individual can prevent himself from malware and banking trojans by avoiding phishing, keeping software update, using security tools, by enabling MFA code and regularly monitoring accounts.

5.3. RANSOMWARE ATTACKS

With over 10% of all the data breeches, ransomware attacks are currently third most popular type of malware. It is type of malware which is used as a tool to pilfer sensitive information and essentially hold it hostage. the data is only released after cyberattackers get ransom payment. Once the ransomware enters into the computer it infects it covertly. The software then attacks files and accesses and modifies the credentials. Consequently, the person who control the malware holds hostage the computer infrastructure.

Preventions Strategies from Ransomware Attacks

Ransomware attacks can be prevented by-

- Keeping devices updated
- Always install software from trusted and verified sources
- Installation of antivirus protection in devices
- Always have Back-Up of data
- Provide training employees

5.4. DATA VULNERABILITY

Data vulnerability is a weakness in system, software or human processes like unpatched software, use of weak passwords or phishing. Data vulnerability allows unauthorised access to sensitive information of individual or corporate.

Preventions Strategies from Data Vulnerability

preventions can be used-

- keep updated software regularly
- Use of strong passwords and MFA
- Provide training to employees
- Limit access user and permissions

5.5. INTERNAL THREATS

Every organisation has people who have authorised access to its system and network these people might be present employees, former staff, consultants, board members or business partners. An insider threat occurs when someone having authorised access uses it to compromise the organisation's cybersecurity intentionally or unintentionally. Insider threats are intentional, unintentional, collusive threats, third party threats and malicious threats.

Preventions Strategies from Insider threats-

- Access control and least privilege
- Implementation of regular monitoring and auditing of user activities
- Deployment of data loss prevention (DLP) tools

6. DATA ANALYSIS AND RESULTS

The incidents of cybercrime in India have increased significantly in the past decade which is due the rapid expansion of digital banking platforms, Mobile payment system and online financial services. As the digital transactions are increasing the cyber criminals are getting more opportunities to take the advantage of loopholes of financial systems. As per the NCRB data 2023-25, India experienced a 31% jump in cybercrimes with over 86000 cases reported.

Table 2

Table 2 Cybercrime and Financial Fraud Cases in India

Year	Reported Cybercrime Case	Financial Fraud Cases	Estimated financial Loss (in ₹ Crore)
2019	44546	12317	1246
2020	50035	14678	1903
2021	52974	16112	2150
2022	65893	18902	2750
2023	71468	21349	3450
2024	80000+	25000+	4000+

Estimated are Based on the Cybersecurity Industry Reports.

Source: NCRB, Cybersecurity Reports by RBI and Cybersecurity Industry Analysis

Figure 1

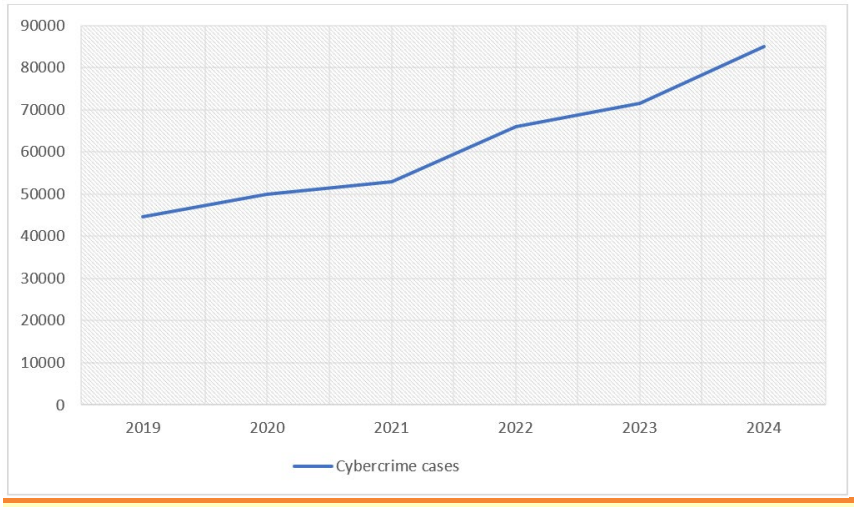

Figure 1 Cybercrime Cases

From the above table and figure it is clear that reported cybercrimes and financial fraud have grown steadily each year. Cybercrime attacks have increased by nearly 80% from 2019 to 2024. This increase reflects the rapid adoption of digital technology and increased use of online platforms, mobile banking and digital payments. Financial fraud cases have also risen sharply, from 12317 in 2019 to more than 25000 in 2024. This increase suggests that cybercriminals are increasingly targeting financial transactions and services and exploiting vulnerabilities in banking and payment system. The financial losses from cybercrime have also increased significantly, from ₹1246 crore in 2019 to an estimated ₹4000 crore in

2024. This increase shows that cybercrimes are not only increasing in volume but their impact and consequences are also becoming more severe.

7. CONCLUSION

In conclusion it is clear that cyber threats to India's digital economy are rapidly increasing. This situation underscores the need for robust cybersecurity measures, stricter regulatory laws, and increased awareness among users and organizations. The rise in financial fraud cases, in particular, indicates that cybercriminals are increasingly focusing on financial systems, requiring the banking and financial sector to strengthen its security. The findings of the study indicates that cybersecuirty has become a critical part of modern banking operations. As cyber threats evolve, financial institutions must adopt proactive and adaptive security strategies. One of the most effective methods of preventing from cyber risk is to implement a multi-layered security architecture that integrates multiple defence mechanisms. These may include firewalls, encryption protocols, intrusion detection system and authentication techniques.

In addition, cybersecurity strategies must also address human factors. Employee training and customer awareness programs are crucial to mitigating vulnerabilities associated with phishing attacks and social engineering.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., and Savage, S. (2019). Measuring the Cost of Cybercrime. Journal of Cybersecurity, 5(1), 1–19.

Arner, D. W., Barberis, J. N., and Buckley, R. P. (2017). FinTech and the Transformation of Financial Services. Journal of Banking Regulation, 19(3), 1–17.

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley. https://doi.org/10.1002/9781119433729

Kshetri, N. (2020). Cybersecurity in the Financial Services Industry. Computer, 53(2), 16–24.

Reserve Bank of India. (2021). Cyber Security Framework for Banks. RBI Publications.

Romanosky, S. (2016). Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

World Economic Forum. (2020). Global Risk Report. World Economic Forum.