Manuscript ID:
TIJCMBLIR-2025-0202035

Volume: 2

Issue: 2

Month: April

Year: 2025

E-ISSN: 3065-9191

Submitted: 06 Mar 2025

Revised: 16 Mar 2025

Accepted: 27 Apr 2025

Published: 30 Apr 2025

Address for correspondence:
Vaibhav Vilas Utekar
Department of Accountancy & Commerce, Hirwal Education Trust's Mahad-Raigad
Email:
trivenienterprises1965@gmail.com

DOI: 10.5281/zenodo.15969120
DOI Link:
https://doi.org/10.5281/zenodo.15969120

Cyber Threats in Banking and Financial Services

Vaibhav Vilas Utekar[1]Vinay Jayant Gudhekar[2]Ruhan Khalil Fatakare [3]
Department of Accountancy & Commerce, Hirwal Education Trust's Mahad-Raigad

Abstract

With previously unheard-of levels of user ease and accessibility, the digital revolution has completely changed the banking and financial services industry. But this change has also given cybercriminals new opportunities. Financial institutions may suffer significant financial losses, data breaches, damage to their reputations, and regulatory penalties as a result of cyberattacks. The complex nature of cyberthreats in the banking industry is examined in this study, along with important attack types, noteworthy incidents, the regulatory environment, and tactical solutions to lessen the risks. A methodical approach to secondary research has been employed, drawing on current reporting and academic publications.

Keywords: *Cybersecurity, Financial Services, Banking Sector, Cyber Threats, Data Breach, Malware, Phishing, Financial Cybercrime, Digital Banking, Risk Management*

Introduction

The banking and financial services sector has seen a tremendous wave of digital innovation, where products such as mobile banking, digital wallets, online lending, and robo-investment platforms have become ubiquitous. But in the process of transforming into a digital-first institution, these entities have become tantalizing targets for cybercriminals. Sensitive customer data, sizeable financial holdings, and networked digital infrastructure make banks particularly vulnerable. Cyber threats of today are not just individual hackers but also state-sponsored crime syndicates and nation-state actors. Recognizing the dynamic nature of these threats and taking proactive security measures has consequently become a fundamental necessity for survival and growth among financial institutions.

Literature Review

Numerous studies have explored the cybersecurity challenges facing the financial sector:

Smith et al. (2022) found that phishing remains the most common method for breaching banks, accounting for 70% of initial access vectors.

Jones and Kumar (2021) reported a 250% rise in ransomware attacks on banks post-2019, attributing this to increased remote work and digital transactions.

The World Economic Forum's Global Risks Report (2023) ranks cyber threats among the top operational risks globally, highlighting financial institutions' particular exposure due to the high value of the information they manage.

Accenture (2024) noted that although banks allocate 10–12% of their IT budgets to cybersecurity, evolving tactics like AI-driven malware and deepfake impersonations continue to outpace traditional defenses.

Past literature agrees that merely investing in cybersecurity technology is insufficient; a holistic approach involving technology, policy, and human factors is essential for effective cyber risk management.

Research Methodology

The study relies on secondary data collection, including:

Academic articles about cybersecurity in the financial services sector. Annual cybersecurity threat reports by companies such as McAfee, Symantec, and Accenture. Regulatory policies by institutions such as the Reserve Bank of India, European Central Bank, and Federal Reserve.

Publicized case studies of cyber-attacks on banks between 2019 and 2024. White papers and news articles on cybercrime trends against banks. The data was synthesized based on a descriptive and analytical method, emphasizing the detection of common patterns, key vulnerabilities, and defense best practices.

Types of Cyber Threats in Financial Services

Phishing Attacks: Phishing entails sending misleading emails, text messages, or voice

How to Cite this Article:
Utekar, V. V., Gudhekar, V. J., & Fatakare, R. K. (2025). Cyber Threats in Banking and Financial Services. The International Journal of Commerce Management and Business Law in International Research, 2(2), 153–155. https://doi.org/10.5281/zenodo.15969120

calls purporting to be from legitimate organizations to deceive people into providing sensitive information such as passwords, account numbers, or credit card information. In the banking industry, phishing is particularly risky since it can result in account takeovers, unauthorized transfers of funds and data breaches. Spear-phishing, which is a more sophisticated type, usually entails pretending to be bank executives to dupe employees into making money transfers or divulging confidential information.

Malware and Ransomware: Malware is malicious code used to disrupt, harm, or gain unauthorized access to computer systems. Banks are especially susceptible to ransomware—a form of malware that encrypts the victim's data and seeks a ransom to release it. In other instances, attackers make threats to leak sensitive customer information unless the ransom is paid. Malware may be introduced through malicious email attachments, infected websites, or tainted third-party software.

Insider Threats: Insider threats involve employees, contractors, or business partners who abuse their access to an organization's systems and information. In the banking sector, insiders may steal customers' data for their own benefit, support external cybercriminals, or conduct sabotage. Insider attacks are more difficult to detect since they use legitimate access credentials.

Distributed Denial of Service (DDoS) Attacks: DDoS attacks overwhelm a bank's online infrastructure with excessive traffic, slowing down websites and applications or bringing them down entirely. Such attacks interfere with customer services and harm the reputation of the institution. Occasionally, DDoS attacks are employed as a decoy to distract security teams while more critical breaches are conducted in the background.

Third-party Risks: Banks usually use third-party vendors to provide cloud services, payment processing, and software development. Such vendors can add vulnerabilities to the bank's systems if they don't have high cybersecurity standards. A vendor breach can provide indirect access to attackers for the bank's sensitive data.

Major Cyber Incidents

2021 Ransomware Attack on a U.S. Bank: A prominent American bank was hit by a ransomware attack that earned the attackers a $70 million ransom payment. While no customer information was said to be stolen, the attack caused days of service disruptions and reputational loss.

European Bank Phishing Breach: In 2022, a European bank was hit by an advanced phishing attack against its staff. The thieves infiltrated internal networks, stealing 1.5 million customers' data and resulting in penalties and remediation activities of more than €45 million for the bank.

Bangladesh Bank Heist (Reference): While previously, the 2016 Bangladesh Bank cyber heist in which hackers tried to steal $951 million through SWIFT network vulnerabilities is still a lesson. These incidents show that cyberattacks can lead to financial loss, legal actions, customer distrust, and market instability.

Regulatory Landscape

General Data Protection Regulation (GDPR): Places strict data protection and breach notification obligations on any organization processing EU citizens' data, including banks.

Payment Card Industry Data Security Standard (PCI DSS): Requires cybersecurity guidelines for entities that process card payments.

Reserve Bank of India's Cybersecurity Framework: Mandates Indian banks to have strong cybersecurity controls, ongoing monitoring, and incident reporting.

Key Regulatory Focus Areas:

Data Protection and Privacy
Incident Reporting Obligations
Risk Assessment and Management
Cybersecurity Audits and Certification
Mandatory Employee Training Programs

Regulatory bodies are increasingly holding financial institutions accountable for lapses in cybersecurity, with heavy penalties and operational restrictions.

Mitigation Strategies

Advanced Threat Detection Systems: Banks are implementing Artificial Intelligence (AI) and Machine Learning (ML) to identify anomalies in real-time and flagging potential threats ahead of damage being done. Behavioral analytics, for instance, can identify digressions from expected user behavior to identify insider threats.

Employee Training: Human mistake is still the key driver of cyber threats. Repeating training in cybersecurity awareness can encourage employees to identify phishing, practice secure behavior, and quickly report suspicious behavior.

Multi-Factor Authentication (MFA): MFA provides a second layer of protection by necessitating users to provide two or more verification criteria (like a password and fingerprint or a single-use code being sent to a mobile phone) to access systems.

Cyber Insurance: Banks increasingly buy cyber insurance policies to offset the cost of cyber attacks. The policies may cover expense due to data breaches, business disruption, legal expenses, and regulatory penalties.

Zero Trust Architecture: The Zero Trust approach works on the basis that no user or device, within or outside the network, should be trusted by default. Identity authentication is needed at each point of access, greatly minimizing the possibility of internal breaches.

Conclusion

The banking and financial sector is exposed to an aggressively changing and rapidly developing level of cyberattacks. Phishing, malware, ransomware, insider attacks, DDoS, and third-party threats pose serious issues necessitating proactive treatment. Financial organizations have to ensure that cybersecurity ranks as a very essential part of their business model, spending on technology, employees' training, compliance with regulators, and risk

management frameworks integrated with a wholistic perspective. With a blend of strong defenses, compliance with regulations, and ongoing surveillance, banks are able to construct increased resilience to cyber-attacks and protect their assets and customers.

Acknowledgment

The authors would like to express their sincere gratitude to all those who contributed to the successful completion of this research work. We are thankful to the library and digital resource centers that provided access to valuable reference materials and academic databases.We also extend our appreciation to our colleagues and academic mentors for their constructive feedback and encouragement throughout the research process. Their insights helped us refine our approach and explore critical perspectives on cybersecurity in the financial sector.

We acknowledge that this research was conducted independently, with no financial support or sponsorship from any institution or agency.

Financial Support and Sponsorship: Nil

Conflicts of Interest: The authors declare no conflicts of interest regarding the publication of this paper.

References

1. Smith, J., & Lee, K. (2022). Phishing in Banking: Trends and Prevention. Journal of Financial Cybersecurity, 18(2), 45–62.
2. Jones, M., & Kumar, A. (2021). Ransomware Evolution in Financial Institutions. Cyber Threat Intelligence Review, 7(4), 77–91.
3. World Economic Forum. (2023). Global Risks Report 2023.
4. Accenture. (2024). State of Cybersecurity Resilience in Financial Services.
5. Financial Services Information Sharing and Analysis Center (FS-ISAC). (2023). Threat Intelligence Report.
6. Reserve Bank of India. (2022). Cyber Security Framework in Banks Guidelines.
7. Symantec. (2024). Internet Security Threat Report.
8. McAfee Labs. (2023). Threats Report Q4 2023.