FROM THEORY TO IMPACT: NEW VISIONS ACROSS DISCIPLINES

FIRST EDITION
2025

Editor-in-Chief
Daniel James

ASDF UK

ISBN 978-81-951337-7-2

From Theory to Impact: New Visions Across Disciplines 2025

FTI 2025

FIRST EDITION 2025

From Theory to Impact: New Visions Across Disciplines 2025

FIRST EDITION FTI 2025

By

ASDF, UK

Financially Sponsored By

Association of Scientists, Developers and Faculties, India

Editor-in-Chief

Daniel James

Editors:

Anbuoli Parthasarathy and Katsuo Shichirou

Published by

Association of Scientists, Developers and Faculties
Address: 483 Green Lanes, London N13 4BS. England. United Kingdom.
Email: admin@asdf.res.in || www.asdf.international

From Theory to Impact: New Visions Across Disciplines 2025 (FTI 2025)

First Edition

Editor-in-Chief: **Daniel James**
Editors: **Anbuoli Parthasarathy and Katsuo Shichirou**

Cover Design: **Saravanan Velayudham**

Disclaimer:

No responsibility is assumed by the FTI 2025 Publisher for any injury and/ or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products or ideas contained in the material herein. Contents, used in the articles and how it is submitted and approved by the contributors after changes in the formatting. Whilst every attempt made to ensure that all aspects of the article are uniform in style, the FTI 2025 Publisher or the Editor(s) will not be responsible whatsoever for the accuracy, correctness or representation of any statements or documents presented in the articles.

ISBN-13: 978-81-951337-7-2
ISBN-10: 81-951337-7-0

Table of Contents

CYBER SECURITY IN FINANCIAL INSTITUTIONS: A FOCUS ON INDIA

S VIGNESWARAN

Assistant Professor, Department of Economics, Mannar Thirumalai Naicker College, Pasumalai, Madurai.

ABSTRACT

Cybersecurity has emerged as a critical concern for financial institutions worldwide, particularly in rapidly digitizing economies such as India. With the exponential growth of digital transactions, online banking, and fintech services, Indian financial institutions are increasingly vulnerable to sophisticated cyber threats. This article delves into the current landscape of cybersecurity within India's financial sector, highlighting prevalent threats, regulatory measures, and technological adaptations. It also discusses the objectives, methodology, and key findings from the analysis while providing suggestions for strengthening cybersecurity frameworks across Indian banks and financial institutions.

Keywords: Cybersecurity, Financial Institutions, Indian Banking Sector, Digital Transactions

INTRODUCTION

The digital transformation of India's financial ecosystem has revolutionized the way banking services are offered and consumed. Services like online banking, mobile wallets, UPI (Unified Payments Interface), and internet-based financial transactions have made financial operations faster and more accessible. However, this evolution has also introduced new vulnerabilities, making financial institutions prime targets for cybercriminals.

India, being home to one of the largest fintech markets in the world, has seen a surge in cyberattacks including phishing, ransomware, DDoS (Distributed Denial of Service) attacks, and data breaches. As per data from the Reserve Bank of India (RBI), the number of reported cybersecurity incidents in banks increased significantly post-COVID-19 due to increased dependence on digital platforms.

OBJECTIVES OF THE STUDY

1. To understand the current cybersecurity landscape in India's financial sector.
2. To identify common cyber threats faced by Indian financial institutions.
3. To evaluate existing cybersecurity frameworks and regulations in India.
4. To suggest strategic measures for improving cyber resilience in financial institutions.

METHODOLOGY OF THE STUDY

The study adopts a **qualitative research methodology** with an exploratory approach. It is based on:

- **Secondary data analysis** from RBI reports, CERT-In advisories, financial sector white papers, and peer-reviewed journals.
- **Case studies** of cyber incidents in Indian banks.
- **Content analysis** of regulatory frameworks such as the RBI's Cyber Security Framework (2016), IT Act 2000, and recent updates from the National Cyber Security Policy.

DISCUSSIONS

1. NATURE OF CYBER THREATS IN INDIAN FINANCIAL INSTITUTIONS

Nature of Cyber Threats in Indian Financial Institutions

Indian financial institutions—ranging from public and private sector banks to cooperative banks and fintech companies—face an evolving and multifaceted range of cyber threats. These threats target not only the technological infrastructure but also exploit human vulnerabilities and regulatory gaps. Below is a detailed breakdown of the key cyber threats:

Phishing and Social Engineering Attacks

Phishing remains the most common and effective method of compromising financial systems. Attackers impersonate legitimate financial institutions via emails, SMS (smishing), or phone calls (vishing), tricking customers and employees into revealing sensitive information like login credentials or OTPs.

- Impact in India: Phishing attacks surged during the COVID-19 pandemic as remote banking increased. According to CERT-In, over 50% of reported financial frauds in 2022 involved phishing techniques.
- Example: Fraudulent links mimicking government-backed schemes or UPI portals have misled customers into disclosing personal data.

Ransomware Attacks

Ransomware involves malicious software that encrypts the victim's data or systems, with attackers demanding ransom payments for restoration. These attacks can paralyze entire banking operations.

- Impact in India: In recent years, several regional cooperative banks and NBFCs (Non-Banking Financial Companies) have reported ransomware attacks due to outdated IT infrastructure.
- Case Highlight: In 2020, a ransomware attack on a large cooperative bank in Maharashtra disrupted online banking for over a week.

ATM Malware and Card Skimming

ATM-related frauds occur through the insertion of malware into ATM systems or physical installation of card skimming devices that clone debit/credit card information.

- Skimming Devices: Hidden cameras or fake keypads capture PINs.
- Malware Attacks: Hackers use external USB drives to inject malware and control ATM cash dispensing mechanisms.
- Impact in India: Skimming-related incidents in cities like Delhi, Mumbai, and Bengaluru have led to losses running into crores of rupees annually.

Distributed Denial of Service (DDoS) Attacks

A DDoS attack overwhelms a bank's servers with a massive volume of traffic, rendering online banking services unavailable.

- Impact: Disruption of critical services such as internet banking, mobile apps, and UPI transactions.
- Trend: Some DDoS attacks are politically motivated or used as a diversion to mask other intrusions.

Insider Threats and Employee Negligence

Internal threats from disgruntled employees or staff members with poor cybersecurity awareness can lead to intentional or unintentional data leaks or system breaches.

- Examples:
    - Sharing passwords or leaving systems unattended.
    - Employees falling for phishing traps and unintentionally granting attackers access to critical systems.
- Risk Factors: Inadequate training, poor access controls, and lack of monitoring.

Data Breaches and Identity Theft

Data breaches involve unauthorized access to customer data including financial records, Aadhaar numbers, PAN, and transaction histories. Such data is often sold on the dark web or used to conduct identity theft.

- Incidents: Multiple Indian banks have experienced customer data leaks, sometimes from third-party service providers like payment gateways.
- Regulatory Repercussions: RBI and SEBI have tightened data protection norms, but breaches still occur, particularly at smaller institutions.

Third-Party and Supply Chain Vulnerabilities

Many banks outsource parts of their IT infrastructure and services (e.g., cloud storage, payment gateways). Cybercriminals often target these third-party vendors who may lack robust cybersecurity controls.

- Risk: A single compromised vendor can lead to data exposure across multiple financial institutions.
- Example: A breach at a cloud-based loan service platform affected numerous NBFCs simultaneously in 2023.

Mobile Banking and App-Based Vulnerabilities

With the explosion of smartphone usage and mobile banking apps, vulnerabilities in app coding, insecure data storage, or outdated app versions have become major targets.

- Issues Identified:
    - Insecure APIs.
    - Lack of encryption.
    - Weak session handling.
- Real-World Impact: Fraudulent apps disguised as legitimate bank apps are used to harvest user credentials.

2. REGULATORY AND INSTITUTIONAL FRAMEWORK

India has initiated several regulatory measures to combat cyber threats:

- **RBI's Cyber Security Framework (2016):** Mandates baseline cybersecurity controls for banks.
- **IT Act 2000 (Amended):** Governs cybercrime and electronic commerce.
- **CERT-In (Indian Computer Emergency Response Team):** Provides real-time incident response support.
- **National Cyber Security Strategy (proposed):** Aims to enhance India's cyber preparedness.

Despite these initiatives, there is inconsistency in implementation across private, public, and cooperative banking institutions.

3. TECHNOLOGICAL ADAPTATION

Banks are increasingly investing in cybersecurity technologies such as:

- AI and ML-based threat detection systems.

- Multi-factor authentication (MFA).
- Real-time fraud monitoring and transaction anomaly detection.
- Blockchain for secure and transparent data handling.

4. CASE STUDIES

A. Cosmos Bank Cyber Heist (2018)

Location: Pune, Maharashtra

Amount Lost: Approx. ₹94 crore (USD 13.5 million)

Type of Attack: Malware Injection and ATM Cloning

Summary:

In one of India's biggest coordinated cyber heists, hackers infiltrated Cosmos Cooperative Bank's server infrastructure and authorized fraudulent withdrawals across 28 countries over two days.

Modus Operandi:

- Malware was injected into the bank's ATM switch server.
- This malware bypassed the Real-Time Gross Settlement (RTGS) system and authorization checks.
- Hackers issued 15,000 cloned debit card transactions through Visa and Rupay card systems.
- Simultaneous ATM withdrawals were conducted globally, including in Canada, Hong Kong, and India.

Impact:

- ₹78 crore withdrawn via 12,000 ATM transactions outside India.
- ₹13.92 crore stolen in India through 2,849 transactions.
- SWIFT-based fraudulent fund transfers were also attempted.
- Massive reputation damage and regulatory scrutiny followed.

Lessons Learned:

- Weak internal monitoring systems and delayed incident detection.
- Highlighted the vulnerability of cooperative banks with outdated IT systems.
- Emphasized the need for network segmentation, 24/7 threat monitoring, and real-time alerts.

2. Canara Bank ATM Server Hack (2016)

Location: Bengaluru

Amount Involved: Over ₹1 crore

Type of Attack: Malware and Unauthorized Server Access

Summary:

Hackers gained unauthorized access to Canara Bank's ATM switch server, enabling them to withdraw cash from ATMs without actual customer debit cards.

Modus Operandi:

- Attackers installed malware on the ATM switch server.
- Fake cards were used to process multiple cash withdrawals.
- Real-time validation was bypassed, and funds were illegally siphoned off.

Impact:

- ₹1 crore was withdrawn fraudulently before detection.
- Systems were temporarily shut down to avoid further compromise.

Lessons Learned:

- Demonstrated the risk of centralized vulnerabilities.
- Highlighted the importance of internal access control and server protection.

3. Union Bank of India SWIFT Breach (2016)

Location: Mumbai (Head Office)

Attempted Theft: USD 171 million

Type of Attack: SWIFT Fraud via Phishing

Summary:

A phishing email targeting a Union Bank employee led to one of the largest attempted cyber thefts in India. Hackers compromised SWIFT credentials and attempted to transfer funds internationally.

Modus Operandi:

- Employee clicked on a malicious link, compromising SWIFT login credentials.
- Hackers initiated unauthorized wire transfers via the SWIFT system to a bank in Cambodia.
- Fortunately, the fraudulent transaction was detected and reversed in time.

Impact:

- Though no funds were lost, the breach highlighted SWIFT-related vulnerabilities.
- The event led to panic across public sector banks, prompting a cybersecurity audit.

Lessons Learned:

- Showed the high-stakes risk of social engineering.
- Necessitated multi-factor authentication and better staff training on phishing awareness.

4. City Union Bank Cyber Attack (2018)

Location: Tamil Nadu

Amount Involved: USD 2 million

Type of Attack: SWIFT Transfer Exploitation

Summary:

Another SWIFT-based breach, this attack targeted Tamil Nadu-based City Union Bank. Cybercriminals attempted to divert funds through intermediary banks in Dubai and Turkey.

Modus Operandi:

- Fraudulent SWIFT messages were sent to transfer large sums.
- Some transactions were flagged and blocked, while others were successfully withdrawn.

Impact:

- Around USD 2 million was at risk, and a portion was lost despite damage control.
- Raised concerns over third-party intermediaries used in fund routing.

Lessons Learned:

- Required end-to-end SWIFT security validation.
- Triggered closer coordination with international banking partners and regulators.

FINDINGS

- Indian financial institutions, especially public sector banks, lag in implementing advanced cybersecurity infrastructure.
- There is a lack of trained cybersecurity professionals within the financial sector.
- Regulatory compliance is often seen as a formality rather than a strategic necessity.
- Customer awareness and education about cyber hygiene remain insufficient.

SUGGESTIONS

1. **Mandatory Cybersecurity Audits:** Periodic assessments by independent cybersecurity firms.
2. **Investment in Cybersecurity Infrastructure:** Upgradation of legacy IT systems and deployment of advanced threat detection tools.
3. **Capacity Building:** Training employees and hiring skilled cybersecurity professionals.
4. **Public Awareness Campaigns:** RBI and banks should launch sustained efforts to educate users.
5. **Inter-agency Collaboration:** Stronger coordination between banks, government agencies, and international cybersecurity bodies.

CONCLUSION

Cybersecurity is no longer a backend IT function but a strategic priority for financial institutions. As India continues its digital banking journey, the robustness of its cybersecurity posture will determine the trust and resilience of its financial system. Financial institutions must evolve from a compliance-based mindset to a risk-based, proactive cybersecurity culture. With continued investment, regulatory support, and stakeholder cooperation, India can build a secure financial ecosystem capable of withstanding future cyber threats.

REFERENCES

1. Reserve Bank of India (2016). *Cyber Security Framework in Banks*.
2. CERT-In. (2023). *Monthly Cybersecurity Reports*.
3. Ministry of Electronics and Information Technology (MeitY). *Information Technology Act, 2000*.
4. KPMG India (2021). *Cybersecurity in Banking Sector: Trends and Insights*.
5. PwC India (2023). *Digital Trust and Cybersecurity in Indian Financial Services*.
6. National Payments Corporation of India (NPCI) Reports, 2022–2024.
7. McKinsey & Company (2023). *The State of Cybersecurity in Indian Finance*.

This article is prepared exclusively for **From Theory to Impact: New Visions Across Disciplines 2025** (ISBN: 978-81-951337-7-2) which is published by ASDF International, registered in London, United Kingdom under the directions of the Editor-in-Chief Dr Daniel James and others of the Editorial Team. Permission to make digital or

ASSOCIATION OF SCIENTISTS, DEVELOPERS AND FACULTIES
483 GREEN LANES, LONDON N13 4BS
INDIA | THAILAND | SOUTH KOREA | UNITED KINGDOM
+44 20 81445548 | ASDF@ASDF.INTERNATIONAL | WWW.ASDF.INTERNATIONAL

£ 99
ISBN 978-81-951337-7-2