DOI: 10.59571/mpi.v3i2.9

Cybersecurity In Banking: The Paradox And The Strategy

Aditi Divatia[i*], Sankalpa Saha, Subhadip Banik & Koustav Kundu

[i]S.P. Jain Institute of Management & Research
* Corresponding author, divatia@spjimr.org

Problem of practice

The digitalisation of banking has not only created unprecedented efficiencies but also amplified cybersecurity risks, making data security a vital concern for financial institutions. As banking transactions migrate to digital platforms, cybercriminals exploit vulnerabilities in banking systems, resulting in financial fraud, data breaches and regulatory non-compliance. The consequences of such breaches extend beyond monetary losses, eroding customer trust and disrupting essential banking operations. Such cybercrimes also result in a paradox, according to the research by Sumit Agarwal, Pulak Ghosh, Tianyue Ruan, and Yunqi Zhang.[1] They demonstrate that while data breaches trigger immediate behavioural shifts in the form of falling digital payment volumes, this effect is short-lived, as consumers ultimately prioritise convenience over security. Thus, the paradox: while security breaches impact customer confidence in the short term, digital adoption remains resilient over time. According to other research by Aitor Couce-Vieira, David Rios Insua, and Alex Kosgodagan, one way to resolve this paradox is for banks to manage cybersecurity risk proactively.[2] Together, these studies underscore the urgency for banking institutions to fortify their cybersecurity infrastructure while maintaining seamless customer experiences. Our essay demonstrates how aligning cybersecurity strategies with emerging technologies, such as artificial intelligence (AI) and blockchain, can enable banks to strengthen their cybersecurity infrastructure while maintaining a seamless customer experience

[1,2] The two articles - 'Transient Customer Response to Data Breaches of Their Information' by Sumit Agarwal, Pulak Ghosh, Tianyue Ruan, and Yunqi Zhang featured in Volume 70, Issue 6 of *Management Science*, and 'Assessing and Forecasting Cybersecurity Impacts' by Aitor Couce-Vieira, David Rios Insua, and Alex Kosgodagan, featured in Volume 17, Issue 4 of *Decision Analysis*, show that the bank data breaches cause short, temporary drops in customer activity and decision-analysis methods can help estimate cyber risks and plan effective responses

From impact to strategy

Cyber threats have become one of the most pressing risks in digital banking. In 2025, global banks were projected to spend USD32 billion on cybersecurity — around 11% of total IT budgets—with major players citing it as their single largest expense.[3] Yet, despite these investments, 80% of bank cybersecurity leaders report being unable to keep pace with and match the intelligence of AI-powered threat actors.[4] This mismatch suggests that growing budgets alone cannot guarantee resilience against increasingly adaptive adversaries.

Implications of the mismatch extend beyond individual institutions. Regulators warn that a successful cyberattack on core banking infrastructure could disrupt essential services such as wage transfers, direct debits and digital payments, with the potential to trigger public panic and systemic instability.[5] The research by Agarwal and team highlights another fallout of cybersecurity breaches: customer trust volatility. Even when actual financial damage is minimal, data breaches create psychological barriers that deter customers from engaging in digital transactions. This is particularly problematic in emerging markets, where the adoption of digital banking is still evolving. Another source of increasing cybersecurity risk is tied to the need to innovate. Many financial institutions rely on open banking ecosystems, where customer data is shared across multiple platforms through fintech collaborations and API integrations. While this enhances financial innovation, these third-party collaborations expose banks to external cyber threats. It also increases the attack surface for cybercriminals.

The above challenges underscore the strategic imperative for banks to move beyond reactive defences and instead adopt proactive, intelligence-driven enterprise cybersecurity strategies.

AI and blockchain

In response to these escalating challenges, the research by Couce-Vieira and team recommends that banks leverage predictive analytics and machine learning to assess cyber risk exposure and forecast potential security incidents. This enables banks to move away from traditional reactive cybersecurity. The following are specific dimensions of enhanced digital security:

Specific dimensions of enhanced digital security:

- AI-driven predictive cyber risk modelling
- Blockchain-enabled tamper-proof audit trails
- Decentralised identity management with AI

AI-driven predictive cyber risk modelling

- Enables proactive anticipation rather than post-incident response.
- Uses machine learning to detect anomalies, malware signatures and unusual transaction patterns.
- Supports resource prioritisation to mitigate financial and reputational damage.
- Examples of advanced threat intelligence tools include **SIEM** (Security Information and Event Management), **OSINT** (Open-Source Intelligence), **Malware Analysis Tools** and **TIPS** (Threat Intelligence Platforms).

Blockchain-enabled tamper-proof audit trails

- Provide immutable, time-stamped records of transactions and security events.
- Reinforce customer trust by securing data integrity and reducing opportunities for tampering.

Decentralised identity management with AI

- Zero-trust security frameworks, which operate on the principle of continuous authentication and verification, can significantly reduce unauthorised access to banking systems.
- Mitigates vulnerabilities in centralised KYC systems by giving customers ownership of their identity data.
- Uses consent-driven smart contracts for selective information sharing.
- Combines AI-driven behavioural biometrics and continuous authentication to enhance fraud prevention.
- Balances strong security with seamless user experience, limiting risks of identity theft.

Collectively, these innovations support a predictive, enterprise-wide cybersecurity framework that moves beyond reactive incident management. Refer to *Figure 1*

for an illustration of how proactive integration can achieve best-in-class security outcomes.

Figure 1: Cybersecurity strategy matrix

	Siloed implementation	Enterprise-wide integration
Reactive approach	**Vulnerable zone** Most small banks; basic firewalls; lack coordinated strategy. High breach risk, slow response time	**Compliance-driven zone** Banks follow minimum regulatory standards; fragmented incident response
Proactive approach	**Tech-driven but disconnected** Advanced tools without alignment across departments; often found in fintechs/startups	**Strategic resilience zone** Large banks with AI-based prediction, board oversight, and integrated risk teams (e.g., JPMorgan, ICICI, SBI)

Source: Created by the authors based on the research by Couce-Vieira, Aitor, David Rios Insua, and Alex Kosgodagan and research by Agarwal, Sumit, Pulak Ghosh, Tianyue Ruan, and Yunqi Zhang

Taken together, these solutions resolve the paradox – they safeguard financial stability while simultaneously sustaining consumer trust in the digital banking ecosystems.

The banker's many roles

Effective cybersecurity management in banking requires active engagement from senior leadership, integrating risk management into the broader business strategy. Traditional compliance-driven models are inadequate for today's dynamic threat environment. To reinforce the conceptual shift from reactive to proactive cybersecurity, banks must redefine the job descriptions, responsibilities and performance metrics of practitioners across functional roles. The following table illustrates how this alignment manifests in leading institutions, such as the State Bank of India (SBI), ICICI Bank and JPMorgan Chase (*see Table* 1). While SBI is India's largest public sector bank with a market capitalisation of over US$95 billion, ICICI Bank is India's largest private bank with a capitalisation of over US$110 billion.[6] JPMorgan Chase is the largest bank in the US, with over US$815 billion in market capitalisation.[7]

Table 1: Functional integration of cybersecurity roles in leading banks

Role	SBI[8]	ICICI Bank[9]	JPMorgan Chase[10]
Customer Relationship Manager (CRM)	• Trained in incident communication protocols and client advisory for secure banking practices • Guides clients on biometric login, multifactor authentication and safe mobile use post-incident • Reinforces trust through proactive engagement	• Guides customers on adopting secure digital habits post-breach via awareness campaigns on multifactor authentication, phishing prevention, and official app use	• Provides role-specific guidance and structured templates for client communication and compensation after breaches • This includes client education resources
IT Officer	• Participates in SBI's internal cybersecurity certification program covering threat intelligence, vulnerability assessment and simulated phishing & denial-of-service drills • Enables predictive, real-time detection and containment	• Conducts 'Red Team' simulations and 'Breach Assessment Exercises' for mission-critical systems • Implements learnings from simulated attacks	• Part of a 1,000+ member cyber team focusing on AI-driven anomaly detection and security operations centre processes • Operates under defined time-to-response service level agreements
Legal Officer	• Cybersecurity governance through data protection and compliance audits • Drafts breach response disclosures aligned to regulatory standards such as GDPR • Oversees data-sharing agreements and regulator coordination	• Manages breach readiness, disclosure, and compensation compliance • Participates in simulated drills per regulatory norms	• Prepares SEC-compliant breach disclosures • Coordinates with IT and public relations for quarterly audits and breach simulations
Credit Officer	• Collaborates with IT for cyber-fraud detection • Trained to identify fraud patterns using anomaly detection in credit scoring and document verification algorithms • Receives red-flag alerts from IT dashboards	• Works with cybersecurity teams to pre-screen suspicious loan applications using incident data	• Uses integrated fraud intelligence for real-time fraud prevention • Flags applications tied to compromised identities, aligned with SOC alerts
Risk Manager	• Integrates cyber risk within the enterprise risk management framework • Conducts cyber incident simulations with functional heads • Reports risk metrics to the board quarterly	• Reviews vulnerabilities in fintech integrations • Updates cyber protocols quarterly through cross-functional collaboration	• Co-develops threat modelling exercises to test exposure to cyberattack scenarios • Outcomes are fed into annual risk appetite recalibration reports

Source: Created by the authors based on corporate websites, as cited in the column headings above

Cross-sector applications

Embedding cybersecurity within enterprise risk governance and transitioning from reactive to predictive frameworks can be extended beyond large banks with adaptations:

- **Medium and small banks:** With appropriate support mechanisms such as cybersecurity co-operatives, managed services and tiered regulatory expectations, even smaller banks can adopt scaled-down versions of predictive and enterprise-integrated cybersecurity frameworks. Budgetary and skill constraints may slow adoption, but the imperative remains both feasible and necessary.
- **Other financial services firms:**
  - *Insurance*: Insurance firms face escalating ransomware and customer data-breach risks. Integrating cybersecurity into enterprise risk frameworks is critical to safeguard data and maintain regulatory compliance.
  - *Wealth & asset management*: These firms handle high-net-worth client data and digital portfolio tools, making them vulnerable to spear-phishing and insider threats. Predictive threat modelling and client education are directly applicable here.
  - *Asset servicing*: Custodians and settlement intermediaries are critical to the financial system. Their reliance on cross-institutional data and APIs makes proactive cybersecurity a systemic requirement.
- **Non-financial services firms:** Sectors such as healthcare, telecom, logistics and retail also manage sensitive data and digital customer interactions. Even though they are subject to lighter regulations, embedding cybersecurity into governance can enhance resilience and trust. However, for firms with lower digital maturity or scale, predictive investments may only be justified where customer trust is central to the business model.

The Capital One breach

The 2019 Capital One data breach serves as a cautionary example of predictable failure arising from weak governance. In this incident, the personal data of over 100 million customers was compromised.[11] Although the proximate cause was a misconfigured firewall, the underlying issue stemmed from the absence of enterprise-wide cybersecurity governance which was capable of detecting systemic vulnerabilities through routine audits.

Capital One's cloud access control policies were not centrally governed, and cybersecurity audits were conducted in silos within IT divisions, without adequate oversight from risk and compliance functions. This structural fragmentation prevented early identification of misconfigurations that could have been mitigated through integrated risk modelling and governance coordination.

The breach ultimately cost Capital One an estimated US$190 million in settlements and regulatory penalties, as well as substantial reputational damage. The incident reinforces the central argument of this essay: cybersecurity cannot remain the sole responsibility of the IT department.

> To reinforce the conceptual shift from reactive to proactive cybersecurity, banks must redefine the job descriptions, responsibilities and performance metrics of practitioners across functional roles. Cybersecurity cannot remain the sole responsibility of the IT department

Investment with impact

The implementation of robust cybersecurity measures is often complicated by regulatory compliance. Financial institutions must navigate complex frameworks such as General Data Protection Regulation(GDPR), PCI-DSS,

and ISO 27001.[12] Ensuring adherence to these frameworks while maintaining operational efficiency can be a daunting task. But banks would also do well to remember that there is an increasing return on these investments of time and money.

Artificial Intelligence (AI) significantly reduces cybersecurity costs through automation, early threat detection and reduced reliance on manual monitoring. AI-driven systems can analyse millions of events in real time, reducing the average breach detection time from months to days or even hours. According to Capgemini Research Institute, organisations that have implemented AI-based cybersecurity solutions reported a 15–20% reduction in operational costs and a 12–15% decrease in breach-related losses.[13]

Examples of AI-based cybersecurity solutions:

- **Automation of threat detection and response** can reduce the workload of human analysts by 30–40%, enabling banks to manage security with leaner teams.
- **Predictive modelling** allows early patching of vulnerabilities, which can reduce remediation costs by up to 25%.
- **AI-powered fraud analytics** can reduce false positives, saving both manpower and customer friction costs.

These savings are particularly valuable for mid-sized banks, allowing them to meet baseline security standards without needing full-scale internal Security Operations Centre (SOC). The above returns are a result of investments, which entail both monetary and non-monetary costs.

Monetary Costs:

- For large banks, implementing AI-driven threat intelligence, zero-trust infrastructure and enterprise governance programs can cost **USD20–50 million** over a three-year transformation horizon.
- Mid-sized banks can leverage shared services and managed SOCs at **USD2–5 million**, using subscription-based cybersecurity solutions.
- Costs may include hardware upgrades, cloud migration, red team services, compliance systems and cyber insurance.

Non-Monetary Costs:

- **Change management resistance:** Institutional inertia, misaligned incentives and lack of cybersecurity literacy can hinder adoption.
- **Customer friction:** While Multi-Factor Authentication (MFA) and secure authentication improve safety, they may increase friction in digital experiences if not designed thoughtfully.
- **Talent constraints:** Recruiting and retaining cyber talent is especially challenging for mid-sized institutions.

Other implementation nuances:

- **Integration complexity:** Retrofitting predictive models into legacy systems can create transitional vulnerabilities.
- **Operational disruption:** Initial deployment phases (e.g., penetration testing, denial-of-service drills) may cause minor service interruptions.
- **Reputational benefit:** Effective implementation can enhance brand equity, especially when proactively communicated to customers and regulators.

Bottom line

While the upfront costs of predictive and AI-driven cybersecurity systems can be substantial, the long-term savings — avoiding breaches, fines and reputational crises — outweigh the initial investment. For banks committed to digital trust and operational continuity, cyber resilience is not just a compliance requirement but a strategic asset.

Cybersecurity in banking requires a multi-layered strategy that integrates enterprise-wide risk management, predictive analytics and proactive customer engagement. Banks must strike a balance between security and convenience, ensuring that stringent security protocols do not compromise the seamless customer experience expected in digital banking environments.

Aditi Divatia *is an Associate Professor of Information Management and Analytics at SPJIMR. You can reach out to her at* ***divatia@spjimr.org***

Sankalpa Saha & Koustav Kundu *are alumni of SPJIMR and currently work at Accenture.* ***Subhadip Banik*** *is an alumnus of SPJIMR and currently works at HSBC*

REFERENCES

[1]Sumit Agarwal et al., "Transient Customer Response to Data Breaches of Their Information," Management Science (Linthicum) 70, no. 6 (2024): 4105, ABI/INFORM Global (3072308211), https://doi.org/10.1287/mnsc.2021.01335.

[2]Aitor Couce-Vieira et al., "Assessing and Forecasting Cybersecurity Impacts," Decision Analysis 17, no. 4 (2020): 356–74, https://doi.org/10.1287/deca.2020.0418.

[3]Kalyeena Makortoff, "'We're Being Attacked All the Time': How UK Banks Stop Hackers," Business, The Guardian, June 15, 2025, https://www.theguardian.com/business/2025/jun/15/uk-banks-hackers-attacks-cybersecurity.

[4]Ilias Tsingenopoulos et al., "On Adaptive Decision-Based Attacks and Defenses," paper presented at 7th Deep Learning Security and Privacy Workshop, DLSP2024 IEEE-Security, IEEE, May 23, 2024, https://dlsp2024.ieee-security.org/papers/dls2024-final24.pdf.

[5]Kalyeena Makortoff, "'We're Being Attacked All the Time.'"

[6]Companies Market Cap, "State Bank of India (SBIN.NS) - Market Capitalization," August 4, 202 AD, https://companiesmarketcap.com/state-bank-of-india/marketcap/; ICICI, "Corporate Governance - Cyber Security," February 27, 2023, https://www.icicibank.com/ms/icici-esg/cyber-security.html.

[7]Companies Market Cap, "JPMorgan Chase (JPM) - Market Capitalization," July 24, 2024, https://companiesmarketcap.com/jp-morgan-chase/marketcap/.

[8]SBI, "Cyber Security - Personal Banking," October 24, 2024, https://sbi.bank.in/web/personal-banking/cyber-security.

[9]ICICI Bank, "Corporate Governance - Cyber Security," Corporate ESG, February 27, 2023, https://www.icicibank.com/ms/icici-esg/cyber-security.html.

[10]JPMC, Item 1C 10-K Cybersecurity GRC, 10-K Cybersecurity GRC (SEC, 2024), 0000019617-24-000225, https://www.board-cybersecurity.com/annual-reports/tracker/20240216-jpmorgan-chase--co-cybersecurity-10k/.

[11]Emily Flitter and Karen Weise, "Capital One Data Breach Compromises Data of Over 100 Million," Business, The New York Times, July 30, 2019, https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.

[12]Anshu Bansal, GDPR vs. HIPAA vs. CCPA vs. PCI: Compliance Differences, Compliance, May 16, 2024, https://www.clouddefense.ai/gdpr-vs-hipaa-vs-ccpa-vs-pci/.

[13]Karine Brunet et al., CRI_AI-and-Gen-AI-in-Cybersecurity_15112024 (CapGemini Research Institute, 2024), https://www.capgemini.com/wp-content/uploads/2024/11/CRI_AI-and-gen-AI-in-cybersecurity_15112024.pdf.

Article Information:
Date article submitted: Jun 3, 2025
Date article accepted: Oct 28, 2025
Date article published: Oct 31, 2025

Images courtesy : www.freepik.com