International Journal of Research in Finance and Management

P-ISSN: 2617-5754
E-ISSN: 2617-5762
IJRFM 2025; 8(1): 789-793
www.allfinancejournal.com
Received: 04-04-2025
Accepted: 08-05-2025

Dr. Nikhil M
Associate Academic Head, International Skill Development Corporation, Kerala, India

Dr. U Sreevidya
Associate Professor, PG and Research Department of Commerce, Government College Malappuram, Affiliated to University of Calicut, Kerala, India

Correspondence Author:
Dr. Nikhil M
Associate Academic Head, International Skill Development Corporation, Kerala, India

Cyber risk management in the financial sector: An evaluation of current practices in modern scenarios

Nikhil M and U Sreevidya

DOI: https://www.doi.org/10.33545/26175754.2025.v8.i1h.508

Abstract
In an increasingly digitized world, the financial sector stands at the forefront of technological advancement and consequently, at heightened risk from cyber threats. The growing complexity of cyberattacks, coupled with the sector's critical role in global economies, demands robust and adaptive cyber risk management strategies. This paper explores the current practices adopted by financial institutions to manage and mitigate cyber risks in modern scenarios. Drawing on recent studies, regulatory guidelines, and institutional case examples, the study identifies prevailing frameworks, tools, and approaches in cyber risk management. The objective is to highlight both strengths and gaps in existing practices, offering insights for strengthening cyber resilience in the financial industry. The findings aim to contribute to ongoing discussions on policy development, organizational preparedness, and the adoption of best practices for managing cyber risks in the evolving threat landscape.

Keywords: Cyber risk management, financial sector, cybersecurity, financial institutions, risk mitigation, cyber resilience, cyber threats, governance, regulatory compliance, digital banking security

Introduction

The digital transformation of the financial sector has brought remarkable benefits in terms of operational efficiency, customer experience, accessibility, and innovation. Technologies such as cloud computing, Artificial Intelligence (AI), blockchain, and mobile banking have reshaped how financial services are designed, delivered, and consumed. According to a 2023 report by Deloitte, over 90% of global financial institutions have accelerated digital adoption post-pandemic to meet changing customer expectations and drive competitive advantage. However, this rapid digitization has significantly expanded the cyber threat surface, exposing financial institutions to unprecedented risks.

Financial institutions are prime targets for cybercriminals due to the sensitive data they handle, including personal information, transaction records, and intellectual property, as well as their critical role in ensuring the stability of national and global economies. The IBM X-Force Threat Intelligence Index 2024 reports that the financial services sector was the most attacked industry for the eighth consecutive year, accounting for nearly 23% of all cyber incidents globally. Ransomware attacks, data breaches, Distributed Denial-of-Service (DDoS) attacks, Advanced Persistent Threats (APTs), supply chain compromises, and sophisticated fraud schemes are increasingly common. The average cost of a data breach in the financial sector reached USD 5.9 million in 2023, significantly above the global average of USD 4.45 million (IBM, 2023) [5].

Given the potential for severe financial loss, reputational damage, regulatory penalties, customer trust erosion, and systemic impacts on the broader financial ecosystem, robust and adaptive cyber risk management has become imperative. Modern financial institutions are expected to go beyond basic compliance and technical safeguards. They must foster a proactive cybersecurity culture, align with evolving regulatory standards, implement comprehensive governance frameworks, and continuously enhance their resilience against emerging threats.

This paper aims to identify and evaluate the existing cyber risk management practices followed by financial institutions in modern scenarios. It examines how these organizations address cyber risks through governance structures, technological controls, risk assessment methodologies, third-party risk management, incident response mechanisms, and employee

awareness initiatives. By assessing these practices, the study seeks to provide a clearer understanding of the sector's cyber resilience, highlight gaps and challenges, and suggest areas where further strengthening may be necessary to protect the integrity and stability of the financial system.

Objectives of the paper

1. To identify the existing cyber risk management practices adopted by financial institutions and evaluate their alignment with regulatory requirements
2. To analyze the effectiveness of cyber risk governance, technology controls, and response mechanisms through recent case examples in the financial sector

Literature Review

Basel Committee on Banking Supervision (2018) [2] emphasizes the importance of cyber resilience as an integral part of operational risk management in financial institutions. However, most studies focus on regulatory expectations rather than institutional implementation practices.

PwC (2021) [15] Global Digital Trust Insights highlights that while 96% of financial institutions increased cyber budgets post-pandemic, few have clear metrics to measure effectiveness of their cyber risk controls. The gap remains in evaluating actual outcomes of these investments.

Accenture (2019) [16] Cost of Cybercrime Study shows that the financial services sector incurs the highest average cost per cyberattack. Yet, little research exists on comparative effectiveness of sector-specific mitigation strategies.

Kopp, Kaffenberger & Wilson (2017) [17] examine systemic cyber risk in the financial sector and warn about contagion effects, but limited studies have analyzed how individual institutions account for these systemic risks in their cyber risk frameworks.

ENISA Threat Landscape Report (2021) [18] provides an overview of threats but does not deeply explore the internal risk management processes financial institutions adopt to respond to these evolving threats.

Deloitte (2020) [19] reports a surge in ransomware and third-party risks. However, there is inadequate academic analysis on how financial institutions are adapting vendor and supply chain cyber risk management practices.

Jang-Jaccard & Nepal (2014) [20] review cyber security issues broadly but provide minimal insight into tailored strategies for financial services, especially in emerging markets.

IMF Working Paper (2020) [21] argues that cyber risk is under-priced in financial risk models, but further empirical research is required on how financial institutions integrate cyber risk into enterprise risk management systems.

IBM X-Force Threat Intelligence Index (2022) [22] identifies insider threats as a rising challenge, yet literature on practical controls and cultural strategies in financial institutions to mitigate these is sparse.

EY (2021) [23] Global Financial Services Information Security Survey highlights a skills gap in cyber talent in financial firms. There is a need for studies examining how institutions are managing this human capital risk within their cyber risk frameworks.

Identified research gap

While there is substantial literature on cyber threats and regulatory guidelines for the financial sector, there is limited empirical research on the actual cyber risk management practices adopted by financial institutions,

Methodology

This study adopts a descriptive research design aimed at analyzing and synthesizing current cyber risk management practices in financial institutions.

Approach

Nature of study: Descriptive

Data type: Qualitative and analytical review of secondary data

Sources of information

Academic journals, white papers, and industry reports

Regulatory and compliance documents (e.g., Basel guidelines, RBI frameworks, EU regulations).

Published case studies and surveys from reputed firms (PwC, Deloitte, Accenture, EY, IBM, ENISA).

News reports and public disclosures on cyber incidents in financial institutions.

Data collection

Systematic review of literature and reports published over the last 10 years.

Thematic analysis of cyber risk management frameworks, practices, and policies documented in secondary sources.

Analysis and Discussion

To identify the existing cyber risk management practices adopted by financial institutions and evaluate their alignment with regulatory requirements.

Cyber risk management has evolved into a strategic priority for financial institutions, driven by escalating threats, regulatory scrutiny, and customer expectations. Unlike conventional IT security, modern cyber risk management in finance is integrated into enterprise risk frameworks and business continuity planning. Regulatory agencies such as the Basel Committee on Banking Supervision (BCBS), Reserve Bank of India (RBI), European Central Bank (ECB), and US FFIEC set comprehensive expectations. These require banks and financial firms to manage cyber risk through proactive identification, protection, detection, response, and recovery capabilities (NIST, 2018) [7].

Common practices in cyber risk management

A review of major global and regional financial institutions reveals the following key cyber risk management practices:

Cyber governance

Board-level oversight: Increasingly, boards have dedicated risk and technology committees overseeing cybersecurity.

CISO leadership: The CISO role is institutionalized, often reporting to the CEO or CRO.

Risk appetite statements: Many institutions define their cyber risk tolerance formally.

Technical controls

- Encryption (at rest and in transit) and data loss prevention systems.
- Multi-factor authentication (MFA) for internal and external access.

- Security information and event management (SIEM) with 24x7 monitoring.
- Penetration testing and red team exercises.
- Endpoint detection and response (EDR) and cloud security tools.

Risk assessment and monitoring
- Regular cyber risk assessments, including vulnerability scans and external audits.
- Threat intelligence sharing via FS-ISAC and national CERTs.
- Third-party risk evaluations (although inconsistent among mid-tier firms).

Incident response
- Documented Incident Response Plans (IRPs).
- Crisis simulations and table top exercises.
- Regulatory reporting (e.g., RBI mandates reporting major incidents within 6 hours).

Human element
- Cybersecurity awareness training, phishing simulations.
- Cultural change programs aimed at embedding cybersecurity consciousness.

Alignment with regulatory requirements

Financial regulators globally emphasize risk-based, rather than purely prescriptive, approaches.

BCBS Principles (2018) [24] require cyber resilience integration into operational risk frameworks.

RBI (2020) mandates robust reporting, threat monitoring, and regular cyber audits.

ECB ICT guidelines stress operational resilience testing, including cyber scenarios.

A 2023 EY Global FS Cybersecurity Survey reported:
- 88% of financial institutions align with ISO 27001/NIST standards.
- 67% updated governance frameworks within 24 months to reflect new regulations.
- However, only 42% perform regular cyber risk assessments of critical third parties.

Similarly, the 2022 PwC Global Digital Trust Insights found 96% of firms increased cybersecurity spending, but only 39% could measure risk reduction effectively.

Strengths and weaknesses identified

Strengths
- Strong technology investments (MFA, SIEM, AI-based fraud detection 82% adoption by large banks, PwC 2022) [9].
- Maturity in incident response planning among tier-1 banks.
- Growing board-level cyber risk oversight.

Weaknesses
- Mid-tier and smaller banks lag in third-party risk management and systemic risk preparation.
- Cultural gaps: Only 39% of EU banks have regular cyber risk sessions for boards (ENISA, 2023) [3].
- Cyber insurance adoption remains uneven, exposing some firms to financial losses.

Bangladesh Bank Heist (2016)

Incident: Attackers compromised Bangladesh Bank's SWIFT environment, stealing USD 81 million via fraudulent transfers.

Root causes: Weak internal controls, outdated firewalls, absence of intrusion detection, untrained staff susceptible to phishing.

Aftermath: SWIFT forced members to adopt stricter controls (Customer Security Programme); regulators globally emphasized SWIFT and payment system security.

To analyze the effectiveness of cyber risk governance, technology controls, and response mechanisms through recent case examples in the financial sector

Cyber governance and technology controls in practice

Cyber governance is the backbone of cyber resilience, linking strategy, accountability, and resources. Effective governance ensures that:
- The CISO has sufficient authority and budget.
- Cyber risk is integrated into enterprise risk management (ERM).
- Boards are informed and involved.

Technology controls, meanwhile, must align with governance strategy
- MFA, encryption, network segmentation, Zero Trust architecture (51% of financial firms now use Zero Trust IBM 2023) [5].
- AI-driven threat detection (82% adoption in large banks PwC 2022) [9].
- Continuous monitoring and real-time incident response.

Capital One Data Breach (2019)

What happened: A misconfigured AWS firewall enabled an attacker to access data of over 100 million customers.

Cause: Weak internal cloud governance; absence of automated configuration audits.

Impact: USD 190 million in penalties and settlements; massive reputational harm.

Lesson: Governance failures can nullify even the most advanced technology controls. Cloud security requires continuous configuration management.

Indian Cooperative Bank Ransomware (2020)

Incident: Ransomware crippled the bank's core banking systems.

Root causes: Lack of network segmentation; no offline backups; absence of a tested incident response plan.

Consequence: Weeks-long service disruption; permanent data loss; loss of customer confidence.

Lesson: Small and mid-tier banks must invest in affordable resilience measures backups, segmentation, and incident planning.

Cross-case insights
- Institutions with strong governance and tested incident response plans (e.g., Singapore's major banks) demonstrate faster recovery, lower losses.
- Technology controls need regular testing, configuration management, and alignment with business processes to be effective.
- Third-party and cloud risks are emerging as significant weak points, requiring focused governance and technical oversight.

Table 1: Cyber risk landscape in financial sector (2023-24)

Metric / Trend	Value / Insight
% of global cyber attacks on finance sector	23% (IBM X-Force, 2024) [6]
Avg. cost of data breach (finance sector)	USD 5.9 million (IBM, 2023) [5]
Adoption of AI fraud detection	82% of large banks (PwC, 2022) [9]
Use of Zero Trust architecture	51% of financial institutions (IBM, 2023) [5]
Institutions aligning with ISO/NIST	88% (EY, 2023) [4]
Regular 3rd party cyber risk assessments	42% (EY, 2023) [4]
Board cyber risk workshops (EU banks)	39% (ENISA, 2023) [3]

Source: Secondary data

Major findings and recommendations

Major findings

1. Cyber risk governance has matured among large financial institutions, but gaps remain in mid-tier and smaller entities. Most tier-1 banks have established dedicated cybersecurity committees, CISO-level leadership, and clear cyber risk appetite statements. However, mid-tier institutions often lack formal governance structures and board-level engagement in cybersecurity oversight.
2. Technology controls are widely implemented but not consistently optimized. Financial institutions have invested heavily in technical controls such as MFA, encryption, SIEM, and AI-based fraud detection. Nevertheless, case studies (e.g., Capital One) show that misconfigurations and poor governance over technology weaken their effectiveness. Cloud and third-party risks remain areas of vulnerability.
3. Incident response capabilities vary significantly across the sector. Large banks generally have well-documented and tested incident response plans, whereas smaller banks often lack regular crisis simulations and offline recovery strategies. This variation was evident in the Indian cooperative bank ransomware incident, where inadequate preparation led to prolonged disruption.
4. Regulatory alignment is strong at policy level but weak in operational execution. While 88% of institutions align with ISO/NIST standards, fewer (42%) perform regular third-party cyber risk assessments, exposing them to supply chain attacks. Board cyber risk awareness training is also limited (39% of EU banks), indicating gaps in embedding cyber resilience into culture.
5. Third-party and cloud service governance is a major weakness. Case examples, including the Capital One breach, highlight that supply chain and cloud risks are not adequately addressed, despite the growing reliance on these services.

Recommendations

1. Enhance cyber governance at all levels of financial institutions. Regulators and boards should mandate structured cyber risk oversight in mid-tier and small institutions, ensuring that cybersecurity is treated as a strategic priority.
2. Strengthen third-party and cloud risk management. Institutions should establish comprehensive third-party risk frameworks, including mandatory periodic audits, configuration management, and continuous monitoring of cloud environments.
3. Increase investment in staff training and cyber culture. Board members, senior executives, and employees require ongoing cybersecurity awareness programs. Institutions should integrate cyber risk awareness into broader corporate culture initiatives.
4. Adopt continuous testing and validation of controls. Financial firms should move beyond periodic audits to continuous control validation, including automated configuration checks, threat simulations, and red team exercises.
5. Focus on systemic risk preparedness. Industry bodies and regulators should promote collaborative cyber resilience exercises simulating sector-wide cyber crises to ensure preparedness for systemic cyber events.
6. Expand cyber insurance coverage prudently. Financial institutions should explore cyber insurance as part of their risk transfer strategy, while carefully evaluating policy scope, exclusions, and claims processes.

Conclusion

The financial sector's rapid digitalization has transformed both service delivery and the cyber risk landscape. This study identified that while significant strides have been made in establishing governance structures, adopting advanced technology controls, and aligning with global standards (e.g., ISO 27001, NIST), critical gaps persist particularly in third-party risk management, cloud security governance, and embedding cyber resilience into organizational culture. The analysis of recent breaches, such as those at Capital One and Bangladesh Bank, illustrates that technology investments alone are insufficient without robust governance, continuous oversight, and a culture of security.

Financial institutions must adopt a holistic approach where governance, technology, processes, and people converge to strengthen resilience against evolving threats. Sector-wide initiatives, regulatory collaboration, and cross-industry exercises are essential to address systemic risks. Future research could further explore the role of emerging technologies like AI-driven threat detection and quantum-resistant cryptography in enhancing the sector's security posture. These findings are consistent with the views presented in key literature, highlighting the need for integrated frameworks (Anderson, 2020; Schneier, 2015) [1, 10] and proactive risk cultures (Von Solms & Van Niekerk, 2013) [12].

References

1. Anderson R. Security engineering: A guide to building dependable distributed systems. 3rd ed. Wiley, 2020.
2. Basel Committee on Banking Supervision. Cyber-resilience: Range of practices. Bank for International Settlements, 2018.
3. European Union Agency for Cybersecurity (ENISA). EU banks cyber resilience report. European Union Agency for Cybersecurity, 2023.
4. Ernst & Young (EY). Global financial services cybersecurity survey. Ernst & Young, 2023.

5. IBM. Cost of a data breach report. IBM Security, 2023.
6. IBM X-Force. Threat intelligence index. IBM Corporation, 2024.
7. National Institute of Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity. NIST, 2018.
8. Pfleeger CP, Pfleeger SL, Margulies J. Security in computing. 5th ed. Pearson, 2015.
9. PwC. Global digital trust insights survey. PwC, 2022.
10. Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company, 2015.
11. Smith RE. Elementary information security. 2nd ed. Jones & Bartlett Learning, 2019.
12. Von Solms R, Van Niekerk J. From information security to cyber security. Comput Secur. 2013;38:97-102. DOI:10.1016/j.cose.2013.04.004
13. Whitman ME, Mattord HJ. Principles of information security. 6th ed. Cengage Learning, 2017.
14. Zhao J, Zhao S. Opportunities and threats: A security assessment of state e-government websites. Gov Inf Q. 2010;27(1):49-56. DOI:10.1016/j.giq.2009.08.002
15. PricewaterhouseCoopers (PwC). Global Digital Trust Insights Survey 2021: Cybersecurity comes of age. PwC, 2021. Available from: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html
16. Accenture, Ponemon Institute. The Cost of Cybercrime Study, 2019. The report highlights that the financial services sector incurs the highest average cost per cyberattack (~US $18.5 million), while research on comparative effectiveness of sector-specific mitigation strategies remains limited. Available from: https://newsroom.accenture.com/news/2019/cost-of-cybercrime-continues-to-rise-for-financial-services-firms-according-to-report-from-accenture-and-ponemon-institute.htm
17. Kopp E, Kaffenberger L, Wilson C. Cyber Risk, Market Failures, and Financial Stability. IMF Working Paper No. 17/185. 2017 Aug 7. International Monetary Fund, 2017. Available from: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104
18. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2021. Athens, Greece: ENISA, 2021 Oct. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
19. Deloitte. Effective Third-Party Risk Management and Governance: Extended Enterprise Risk Management Survey 2020. Deloitte, 2020. The report highlights a surge in ransomware and third-party risks, noting that only 44% of institutions consider themselves “extremely or very effective” in managing these risks, and points to inadequate academic analysis of how financial institutions adapt vendor and supply chain cyber risk practices. Available from: https://www2.deloitte.com/us/en/pages/risk/articles/third-party-risk.html
20. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J Comput Syst Sci. 2014 May;80(5):973-793. Available from: https://doi.org/10.1016/j.jcss.2014.02.005
21. Goh J, Kang H, Xing Koh Z, et al. Cyber Risk Surveillance: A Case Study of Singapore. IMF Working Paper No. 20/028. International Monetary Fund, 2020 Feb 10. Available from: https://www.imf.org/-/media/Files/Publications/WP/2020/English/wpiea2020028-print-pdf.ashx
22. IBM Security. X-Force Threat Intelligence Index 2022. IBM, 2022. The report highlights a rise in insider threats, but points out that literature on practical controls and cultural strategies in financial institutions is limited. Available from: https://www.ibm.com/reports/threat-intelligence/2022
23. EY. Global Information Security Survey 2021. London: EY, 2021. The survey highlights a skills gap in cyber talent at financial firms and calls for studies on how these institutions manage such human capital risk within their cyber risk frameworks. Available from: https://www.ey.com/en_ca/insights/cybersecurity/global-information-security-survey-2021
24. Basel Committee on Banking Supervision. Cyber-resilience: range of practices. Basel: Bank for International Settlements, 2018 Dec. The report emphasizes that cyber resilience should be integrated into financial institutions' operational risk frameworks. Available from: https://www.bis.org/bcbs/publ/d454.pdf