www.ijarp.com ISSN 2456-9992 Page: 01-07

International Journal Advanced Research Publications

Research Article

Volume: 02
Issue: 11

CYBERSECURITY RISK AND FINANCIAL STABILITY OF INDIAN BANKING INSTITUTIONS – AN EMPIRICAL ASSESSMENT OF SELECTED INDIAN COMMERCIAL BANKS

***J. Lavanya**

Associate Professor, Badruka College of Commerce and Arts, Hyderabad, India.

Article Received: 02 October 2026, Article Revised: 21 October 2026, Published on: 11 November 2026

***Corresponding Author: J. Lavanya**

Associate Professor, Badruka College of Commerce and Arts, Hyderabad, India.

Doi: https://doi-doi.org/101555/ijarp.4939

ABSTRACT

The rapid digitisation of Indian banking has increased the strategic importance of cybersecurity, information security, operational resilience and data protection. This study examines whether the quality and breadth of cybersecurity-related disclosure are associated with selected indicators of financial stability among major Indian commercial banks. The study uses a FY2024–25 cross-sectional sample of ten large public and private sector banks. A preliminary Cybersecurity Disclosure Index (CDI) is constructed from annual-report disclosures covering governance, cyber policy, security operations, incident response, vulnerability testing, employee awareness, third-party risk and certifications. Financial outcomes include return on assets (ROA), return on equity (ROE), net non-performing assets (NNPA) and capital adequacy ratio (CRAR). Pearson correlations and exploratory OLS regressions are reported. The evidence indicates a positive association between cybersecurity disclosure and ROA, while the relationship with ROE is weaker and the relationship with NNPA is negative. The findings should be interpreted as associations rather than causal effects because cybersecurity disclosure is an imperfect proxy for underlying cyber risk and the sample is cross-sectional. The study provides a replicable framework for a larger five-year panel once bank-level cyber-incident and expenditure data are consistently available.

KEYWORDS: Cybersecurity Risk; Financial Stability; Indian Banks; Cybersecurity Disclosure; ROA; ROE; NPA; CRAR; Digital Banking.

1. INTRODUCTION

Indian banking has become increasingly dependent on digital channels, cloud infrastructure, application programming interfaces, mobile applications and real-time payment systems. This digital dependence creates operational benefits but also exposes banks to cyber threats, data breaches, service disruption, and fraud and third-party technology risks. The Reserve Bank of India (RBI) has treated cyber/IT risk as a significant operational risk and has continued to strengthen cyber resilience, incident monitoring, fraud detection and supervisory assessment. The RBI Annual Report 2024–25 specifically identifies cyber security as an ongoing supervisory priority and notes work on thematic cyber-risk reviews, cyber mapping and market-wide cyber crisis simulations.

The financial consequences of a material cyber event can extend beyond direct monetary losses. Operational downtime can interrupt payments and lending services; customer-data incidents can affect trust; fraud losses can increase provisions; and persistent technology weaknesses can create regulatory, legal and reputational costs. Consequently, cybersecurity can be viewed as part of the broader financial-stability architecture of a bank.

2. Regulatory and Institutional Context

RBI's supervisory framework requires regulated entities to strengthen information-security governance, cyber-risk management, incident reporting, audit and resilience. The RBI Annual Report 2024–25 states that cyber security continued to be assessed as a major operational risk and reports enhanced supervisory work on cyber resilience and cyber-risk assessment. This institutional context supports examining cybersecurity alongside conventional indicators of bank stability.

3. Review of Literature

Bouveret (2018) highlighted that cyber incidents can create financial losses, fraud and business disruption in the financial sector. Aldasoro et al. (2020) found that cyber losses can form a significant component of operational risk in large banks. The Basel Committee on Banking Supervision (2021) emphasised governance, ICT resilience, incident management and business continuity as essential elements of banking resilience. Doerr et al. (2022) identified cyber risk as an important concern for financial institutions and central banks, particularly because of the potential for wider financial-system effects. More recent BIS and FSI studies (2026) have shown that cyber stress testing and supervisory attention can strengthen banks' cybersecurity preparedness and investment. Overall, the literature indicates

that cybersecurity is closely linked with operational resilience and financial stability; however, comparable bank-level data on cyber incidents, expenditure and losses remain limited. Therefore, the present study uses a **Cybersecurity Disclosure Index** as a transparent proxy to examine its relationship with **ROA, ROE, Net NPA and CRAR** of selected Indian banks.

4. OBJECTIVES

1. To examine cybersecurity-related disclosure practices among selected Indian commercial banks.
2. To analyse the association between cybersecurity disclosure and bank profitability.
3. To examine the relationship between cybersecurity disclosure and asset quality.
4. To assess whether cybersecurity disclosure is associated with capital adequacy.
5. To develop a replicable empirical framework for future multi-year research on cyber risk and bank stability.

5. Hypotheses

H1: Cybersecurity disclosure is positively associated with ROA.

H2: Cybersecurity disclosure is significantly associated with ROE.

H3: Cybersecurity disclosure is negatively associated with Net NPA.

H4: Cybersecurity disclosure is positively associated with CRAR.

6. Sample and Data

The sample comprises ten major Indian commercial banks: State Bank of India, HDFC Bank, ICICI Bank, Axis Bank, Kotak Mahindra Bank, IndusInd Bank, Bank of Baroda, Punjab National Bank, Canara Bank and Union Bank of India. The empirical window is FY2024–25. Financial indicators were taken from bank annual reports and official financial results where available. Cybersecurity disclosure was coded from publicly available annual-report disclosures.

Important scope note: a comparable five-year institution-level cybersecurity-loss series is not consistently reported by Indian banks. Therefore, the present version is deliberately a FY2024–25 cross-sectional pilot rather than an artificial FY2020–21 to FY2024–25 panel. This avoids inventing cyber-incident or cybersecurity-spending observations.

7. Variable Measurement.

Variable	Measurement	Operational definition
Cybersecurity Disclosure Index (CDI)	0–8 score	One point for each documented disclosure dimension.
ROA	Percentage	Return on Assets.
ROE	Percentage	Return on Equity.
Net NPA	Percentage	Net Non-Performing Assets ratio.
CRAR	Percentage	Basel III Capital to Risk-Weighted Assets Ratio.

8. Cybersecurity Disclosure Index

The CDI contains eight disclosure dimensions: (1) board/management cybersecurity oversight; (2) board-approved cyber/information-security policy; (3) dedicated security operations or monitoring capability; (4) incident-response or cyber-crisis management; (5) vulnerability assessment/penetration testing; (6) employee/customer cybersecurity awareness; (7) third-party/vendor technology-risk controls; and (8) information-security certification or recognised security standards. Each disclosed dimension receives 1 point; otherwise 0. The resulting score ranges from 0 to 8.

The CDI measures disclosure breadth, not the true probability or severity of cyber attack. A higher score therefore means broader documented cybersecurity governance and controls, not necessarily higher or lower realised cyber risk.

9. Empirical Dataset: FY2024–25

Bank	CDI	ROA %	ROE %	Net NPA %	CRAR %
State Bank of India	7	1.10	19.87	0.47	14.25
HDFC Bank	8	1.60	13.70	0.43	19.40
ICICI Bank	8	2.40	17.80	0.40	16.55
Axis Bank	8	1.77	16.89	0.33	17.07
Kotak Mahindra Bank	8	2.21	12.57	0.31	22.20
IndusInd Bank	7	0.50	4.17	0.95	16.24
Bank of Baroda	6	1.16	16.96	0.58	17.19
Punjab National Bank	6	0.97	19.33	0.40	17.01
Canara Bank	6	1.09	21.28	0.70	16.33
Union Bank of India	8	1.26	17.20	0.63	18.02

10. Descriptive Statistics

Variable	N	Mean	Std. Dev.	Minimum	Maximum
Cybersecurity Disclosure Index	10	7.200	0.919	6.000	8.000
ROA	10	1.406	0.586	0.500	2.400
ROE	10	15.977	4.914	4.170	21.280
Net NPA	10	0.520	0.198	0.310	0.950
CRAR	10	17.426	2.131	14.250	22.200

11. Correlation Analysis

Outcome	Pearson r with CDI	p-value
ROA	0.662	0.037
ROE	-0.280	0.434
Net NPA	-0.379	0.280
CRAR	0.446	0.196

12. Exploratory Regression Results

Dependent variable	CDI coefficient	Robust SE	p-value	R^2
ROA	0.4221	0.1286	0.0010	0.438
ROE	-1.4953	0.9853	0.1291	0.078
Net_NPA	-0.0816	0.0535	0.1276	0.143
CRAR	1.0339	0.5967	0.0831	0.199

The exploratory estimates indicate that CDI is positively associated with ROA, while the association with ROE is negative in this small cross-sectional sample. CDI is negatively associated with Net NPA and positively associated with CRAR. Statistical significance should be interpreted cautiously because the sample contains only ten banks, the CDI is disclosure-based, and no full set of bank-level controls is included.

13. DISCUSSION

The positive association between cybersecurity disclosure and ROA is consistent with the possibility that stronger technology governance accompanies better operational discipline and resilience. The negative association between CDI and Net NPA is also compatible with the idea that stronger digital controls can support fraud prevention and operational risk management. These interpretations are hypotheses rather than causal conclusions. Cybersecurity disclosure may also be correlated with bank size, regulatory scrutiny, technology investment, governance quality and digital maturity.

The evidence from individual banks illustrates the heterogeneity of cyber-governance practices. For example, HDFC Bank's FY2024–25 annual report describes a dedicated Cyber Security Operations Center, penetration testing, attack-surface management, SOAR and AI/ML-enabled monitoring. Axis Bank reports multi-layered security architecture, AI-driven threat detection and cyber-security awareness initiatives. Kotak Mahindra Bank reports board-approved cybersecurity policy, vendor security assessments, a three-line defence model and ISO/IEC 27001 certification. Union Bank reports a Cybersecurity Centre of Excellence, monthly phishing simulations, a 24x7 Cyber Security Operations Centre and ISO certifications.

14. Limitations

- The sample contains ten banks and one financial year, limiting statistical power.
- The Cybersecurity Disclosure Index is a proxy for disclosure breadth, not realised cyber loss or attack probability.
- Banks may differ in reporting style; absence of disclosure does not prove absence of a control.
- The analysis does not establish causality.
- A stronger five-year panel requires consistent institution-level cyber incidents, cyber expenditure, cyber-loss or comparable risk indicators.
- Future research should add bank size, digital transaction intensity, leverage, liquidity, cost-to-income ratio and governance controls.

15. CONCLUSION

Cybersecurity has become an integral component of banking resilience in India's increasingly digital financial system. The FY2024–25 evidence in this pilot study shows measurable associations between cybersecurity disclosure and selected financial indicators, particularly ROA, Net NPA and CRAR. The findings support continued empirical investigation but should not be interpreted as proof that cybersecurity disclosure itself causes stronger financial performance. A future five-year panel using standardised cyber-risk measures would provide a substantially stronger basis for fixed-effects, random-effects and Hausman-test analysis.

16. Data Integrity Statement

No cybersecurity incident counts, cybersecurity expenditure or five-year cyber-risk observations have been fabricated. Where comparable bank-level cyber-risk data are not publicly standardised, the study uses a clearly identified disclosure proxy. The accompanying CSV contains the FY2024–25 empirical dataset used for the exploratory calculations.

REFERENCES AND PRIMARY SOURCES

1. Reserve Bank of India (2025). Annual Report 2024–25, Chapter VI: Regulation, Supervision and Financial Stability.
2. State Bank of India (2025). Annual Report 2024–25.
3. HDFC Bank (2025). Integrated Annual Report 2024–25.
4. Axis Bank (2025). Integrated Annual Report 2024–25.
5. Kotak Mahindra Bank (2025). Integrated Annual Report 2024–25.

6. IndusInd Bank (2025). Integrated Annual Report 2024–25.
7. Union Bank of India (2025). Integrated Annual Report 2024–25.
8. Bank of Baroda (2025). FY2024–25 financial results / annual reporting disclosures.
9. Punjab National Bank (2025). Annual Report 2024–25.
10. Canara Bank (2025). Annual Report 2024–25.
11. ICICI Bank (2025). Annual Report FY2025.