



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

The Adoption and Organisational Impact of AI-Driven Cybersecurity Solutions: A TOE–Trust Integrated Model with Evidence from Business Organisations and Listed Companies

Alexandre Davitaia¹, Dhrobajoti Paul²

¹Independent Researcher, Germany. Email: leksodav@proton.me

²Cyber Security and Digital Forensics Indian Institute of Information Technology (IIIT) Kottayam. E-mail: dhrobajoti.kiit@gmail.com, ORCID: 0009-0005-5031-6227

Abstract

The adoption of Artificial Intelligence (AI)-based cybersecurity is becoming an essential component of organisational resilience, but evidence on the drivers and impacts of AI-based cybersecurity adoption is limited and largely composed of primary or secondary data sources only. This study combines the Technology–Organisation–Environment (TOE) framework with Trust theory to investigate the adoption of AI in the context of cybersecurity in ten top Indian listed financial organizations. A structured questionnaire was sent to managers, IT security experts, and employees who provided 200 responses from which 164 were obtained after data screening. The results indicate that Technological Readiness ($\beta=.291, p<.001$) and Organisational Capacity ($\beta=.256, p<.001$) both significantly and positively affect organisational performance, whereas Environmental Pressure ($\beta=.111, p=.057$) has a positive but non-significant effect. Organisational Trust partially mediates the TOE–Performance relationship (indirect effect=.202, 95% CI [.116, .304]). A mean score analysis was conducted to compare the extent of disclosure of private banks with NBFCs and the sampled insurer based on a scorecard using an AI-Driven Cybersecurity Disclosure Index (ADCI) derived from their Annual Reports and BRSR filings, and the private banks scored higher at 6.6/20 compared to the NBFCs and sampled insurer. Notably, environmental/regulatory factors impacted corporate disclosure but not individual level perceptions of adoption, pointing to technological capability, organisational support and trust as key factors in successful adoption of AI in the cybersecurity space.

Keywords: AI-driven cybersecurity; TOE framework; organisational trust; technology adoption; BRSR disclosure; mediation analysis

1. Introduction

1.1 Background of the Study

In the last decade, cybersecurity threats have become much more sophisticated and cleverer, with attackers relying more on automation and machine learning to create attacks that move faster than the rule-based defence mechanisms can keep up. Structural limitations prevail in this environment as static security systems are only able to identify attacks if they have been previously programmed with a signature. It has driven organisations toward AI-based cybersecurity solutions, such as machine learning-based behavioural anomaly detection, automated threat response, and predictive risk scoring, all of which are aimed at, and adapt to, threats, not just those that are known.

The two structural changes have been contributing to this shift; first, the widespread move to cloud infrastructure and remote work has expanded the number of potential entry points available to attackers, increasing the monitoring burden on security teams. Second, regulators across sectors have progressively tightened expectations around demonstrable cyber-resilience, meaning organisations must not only be secure but be able to formally evidence that security through governance structures and disclosure.

Financial services offer a particularly instructive setting for studying this phenomenon. Financial institutions hold highly sensitive personal and transactional data, making cybersecurity a business-critical concern rather than a peripheral IT function. The sector is also subject to some of the most stringent, sector-specific regulatory oversight globally — in India, this includes the RBI for banks, SEBI for listed companies broadly, and IRDAI for insurers — producing measurable variation in regulatory intensity across financial sub-sectors. This variation is what allows the present study to examine whether environmental/regulatory pressure operates consistently across both individual-employee perception and institutional-disclosure behaviour, or whether — as this study's findings suggest — the two diverge.

1.2 Problem Statement

Existing research splits into two disconnected traditions: primary, perception-based studies of adoption intent, and secondary, archival studies of disclosed cybersecurity posture. No study has combined both — from the

same organisations, within one theoretical model — to test whether individual perception and institutional disclosure align. This study addresses that gap.

The gap identified above is threefold. Empirically, no prior study pairs primary adoption-perception data with secondary disclosure data from the same organisational sample. Theoretically, no reviewed TOE application formally tests trust as a mediating mechanism specific to AI-driven cybersecurity. Methodologically, no study has demonstrated whether individual-level and institutional-level expressions of environmental pressure converge or diverge. This study's novelty lies precisely in closing all three gaps simultaneously through a single triangulated design, and its contribution is a validated, replicable template — pairing SPSS-based primary analysis with an independently constructed disclosure index — for testing alignment between organisational perception and organisational behaviour in future AI-governance research.

1.3 Research Objectives

- To examine the influence of Technological, Organisational, and Environmental (TOE) factors on the adoption of AI-driven cybersecurity solutions.
- To evaluate the impact of AI-driven cybersecurity adoption on organisational performance.
- To investigate the mediating role of organisational trust in the relationship between TOE factors and organisational performance.
- To triangulate primary survey findings against secondary disclosure-based evidence (ADCI) from the same sampled companies.

1.4 Research Questions

- RQ1: How do TOE factors influence AI-driven cybersecurity adoption?
- RQ2: Does organisational trust mediate the TOE–performance relationship?
- RQ3: Does employee-perceived adoption align with company-level disclosure behaviour?

1.5 Significance of the Study

Theoretically, the study extends the TOE by explicitly addressing the pathway of mediation of trust in AI cybersecurity contexts. In terms of method, it has a triangulated design, with primary survey data compared with secondary disclosure metrics built independently by the same firms. In practical terms, it provides financial-sector regulators and governance practitioners with evidence of the intersection and space between employee perception and formal disclosure

1.6 Scope and Limitations

The study is delimited to ten financial companies that are part of the Nifty Financial Services Index, and have been selected through purposive, criterion based sampling in consideration of mandatory BRSR and top 10 companies based on market-cap. This results in a sample that is biased toward banks and includes little representation of insurance and no representation of asset management. The data is fully verified for FY24-25, and only partially verified for the two previous years of data coverage, which is clearly stated in Section 5.4 rather than camouflaged.

2. Literature Review

2.1 AI Adoption in Organisational Contexts

Adoption literature in the field of General AI sets internal organisational ability as more likely to predict successful adoption than external environmental pressure. In the study of more than 12,000 European SMEs by Arroyabe et al. (2024), external environment support was found to be lower than internal digital capability. Badghish and Soomro (2024) validated the drivers of adoption as compatibility and government support, also firm size moderated the adoption–performance relationship. Among SMEs that are adopting AI at a broader level, Sánchez, Calderón and Herrera (2025) reported that cybersecurity concern was identified as one of the major environmental barriers.

Critical summary: This literature is largely SME-oriented and adoption dynamics of large firms are generally not examined, particularly in the context of sector-specific factors relevant to services industries that are regulated in a stricter manner than other sectors, such as financial services, which are studied directly in this paper.

2.2 The TOE Framework

The TOE framework proposed by Tornatzky and Fleischer (1990) provides a broader explanation of technology adoption by considering three environments: technological, organisational and environmental. This framework has been extended to the enterprise technology adoption, in general (Oliveira & Martins, 2011).

2.3 Trust in Automated and AI Systems

Mayer, Davis, and Schoorman (1995) refer to trust as equal to perceived ability, benevolence, and integrity, while McKnight, Choudhury, and Kacmar (2002) add "trust in technology" in which the trusted person is an algorithmic system. AI-powered cybersecurity solutions make it even harder: the greater the trust they require, the less they can be relied upon to work correctly.

2.4 AI-Driven Cybersecurity Adoption

The study by Nadella et al. (2024) showed good predictive efficiency of machine learning-based threat classification in SME contexts, but this study did not directly study the drivers of organisational adoption. In this study, we found that Technological Readiness is the most important deployment barrier, similar to the one identified in the Ponemon Institute (2024) which surveyed 641 security practitioners, with legacy-system

interoperability as the top deployment barrier. This study and the sample of financial institutions reflect that larger financial institutions are leading the adoption of AI-cybersecurity, as evidenced in KPMG (2025).

2.5 Disclosure, Governance, and Organisational Performance

SEBI's BRSR mandate has institutionalised cybersecurity and data-governance disclosure among large listed Indian companies, providing a structured basis for linking disclosed cybersecurity posture to financial performance — the empirical foundation for this study's secondary-data layer.

2.6 Synthesis and Research Gap

Across these five themes, no reviewed study integrates TOE-based adoption theory, formal trust-mediation, and disclosure-based secondary evidence within a single design applied to an identical organisational sample. This is the specific contribution advanced here.

3. Research Methodology

3.1 Research Design

This study adopts a mixed-method, cross-sectional research design, combining quantitative primary research (a structured questionnaire survey) with quantitative secondary research (archival analysis of company disclosures and financial performance). Primary data were collected at a single point in time, while the secondary layer draws on three retrospective fiscal years — FY 2022-23, FY 2023-24, and FY 2024-25 — with the ADCI disclosure index scored only for the most recent, fully verified year. This dual-layer structure enables the study's central contribution: triangulating individual-level perception against organisational-level disclosure behaviour.

3.2 Population and Sample

The main population consisted of managers, IT security experts and staff from the listed financial companies in India who have access to AI-based cybersecurity solutions. Secondary population consisted of listed Indian financial companies that are required to file BRSR under SEBI regulations.

Ten companies were purposively and criterion sampled based on their membership in Nifty Financial Services Index, BRSR filing status and top ten companies in terms of Free Float Market Cap.

Table 1: Sample Companies and Index Weightage

Company	Sub-Sector	Weightage (%)
HDFC Bank	Private Bank	32.54
ICICI Bank	Private Bank	21.97
Axis Bank	Private Bank	7.32
Kotak Mahindra Bank	Private Bank	6.93
State Bank of India	PSU Bank	6.86
Bajaj Finance	NBFC	5.42
Bajaj Finserv	NBFC	2.43
Jio Financial Services	NBFC	2.33
Shriram Finance	NBFC	2.15
HDFC Life Insurance	Insurance	~2.00

The 36 respondents who showed minimal difference across all items on the Likert scale were removed and 164 of the 200 primary responses remained to form the sample. This sample size is large enough to meet the minimums for regression with three predictors (Green's rule: at least 74) and for medium effect size at conventional power (G*Power calculations: a minimum of about 77). Net Profit verified for all 3 years and all 10 companies, Total Assets verified (4 of 30), ADCI scores verified for all 10 companies for FY 2024-25 with confidence levels noted by company in Section 4.8.

3.3 Data Collection

Primary data were collected via a structured, self-administered questionnaire distributed to managers, IT/security professionals, and employees across the ten sampled organisations, completed as a single cross-sectional exercise. 200 responses were received; 164 were retained after screening (Section 3.2).

Secondary data were collected through documentary retrieval from each company's official Annual Reports, BRSR filings, and press releases. Financial figures (Net Profit, Total Assets) were cross-checked against a second source where available; ADCI content was obtained by scoring each company's disclosures against the ten-item checklist.

3.4 Hypotheses

- **H1:** Technological Readiness (TECH) positively influences Adoption/Performance (PERF).

- **H2:** Organisational Capacity (ORG) positively influences PERF.
- **H3:** Environmental Pressure (ENV) positively influences PERF.
- **H4:** Organisational Trust (TRUST) mediates the relationship between TOE factors and PERF.

3.5 Analytical Procedure and Statistical Tools

Primary data were analysed through a sequential pipeline: reliability testing (Cronbach's Alpha), Exploratory Factor Analysis with Varimax rotation (supported by KMO and Bartlett's Test), descriptive statistics and Pearson correlation, multiple regression (supported by VIF and Durbin-Watson diagnostics) to test H1–H3, and Hayes' PROCESS macro (Model 4, 5,000 bootstrap resamples) to test H4. PROCESS Model 4 was selected as the standard model for simple single-mediator mediation matching this study's theorised structure; Varimax rotation was selected on the assumption that the five constructs represent conceptually distinct factors intended for use as independent variables in regression. Secondary data were analysed descriptively at company level, serving a triangulation function against primary findings in Section 4.8 rather than independent hypothesis testing.

Statistical tools used: IBM SPSS Statistics (Version 26 or later) was used for all primary data analysis — reliability testing, EFA, descriptive statistics, correlation, multiple regression, and PROCESS-based mediation analysis. Python (NumPy, Pandas, SciPy, Statsmodels) was used to independently cross-verify SPSS outputs and to compute bootstrap confidence intervals for the mediation analysis. Microsoft Excel was used for organising and structuring the secondary dataset (ADCI scoring sheet and financial performance sheet) prior to analysis.

4. Results and Analysis

4.1 Primary Data Analysis

This sub-section (4.2–4.8) reports the analysis of primary survey data collected from 164 respondents, covering sample profile, reliability, validity, descriptive and inferential statistics, and hypothesis testing.

4.2 Sample Profile

Table 2: Respondent Demographic Profile (N = 164)

Category	Group	%
Gender	Male	53.0
	Female	43.3
Age	31–40	39.6
	21–30	33.5
Designation	IT/Security Manager	23.8
	General Employee	18.9

Result: The sample is fairly gender, age and role representative, so findings are unlikely to be from one perspective within the organisation.

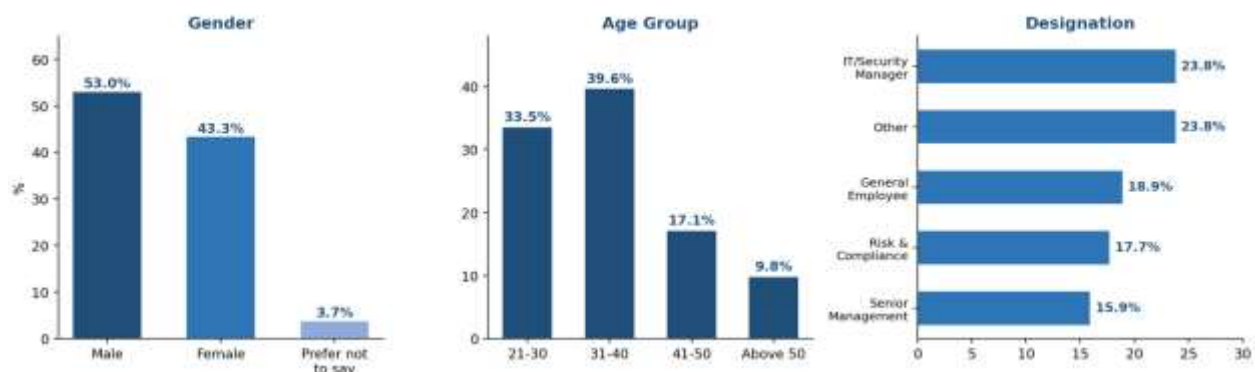


Figure 1: Respondent Demographic Profile (N = 164)

4.3 Reliability Analysis

Cronbach's Alpha can be used to assess internal consistency, that is, whether items are measuring the same construct and will be correlated. $\alpha \geq .70$ suggests that the items are measuring one consistent construct.

Table 3: Construct Reliability

Construct	α
TECH	.831

Construct	α
ORG	.859
ENV	.812
TRUST	.804
PERF	.799

Result: All five constructs have values over .70 indicating that these 25 survey items measure their intended constructs before further analysis.

4.4 Exploratory Factor Analysis

EFA with Varimax rotation assesses if items statistically cluster into the a priori number of constructs. Sample adequacy: .60 or higher is acceptable (KMO test); Bartlett's Test: $p < .05$ required, indicating meaningful correlation among items.

Table 3a: EFA Factor Loadings (Varimax Rotated)

Item	F1 (PERF)	F2 (ENV)	F3 (ORG)	F4 (TECH)	F5 (TRUST)
TECH1	.151	-.109	.079	-.730	.238
TECH2	.087	.004	.201	-.726	.202
TECH3	.305	.015	.077	-.728	.003
TECH4	.171	-.230	.043	-.704	.136
TECH5	-.012	-.057	.127	-.768	.144
ORG1	.214	-.009	.746	-.204	.185
ORG2	-.005	-.039	.805	-.151	.054
ORG3	.155	.052	.781	.026	.201
ORG4	.054	.002	.775	-.048	.072
ORG5	.240	.052	.729	-.122	.163
ENV1	.097	-.801	-.005	-.020	.010
ENV2	-.009	-.791	-.049	-.025	.123
ENV3	.017	-.691	-.075	-.158	-.132
ENV4	.123	-.784	.025	-.115	-.070
ENV5	.057	-.674	.071	-.012	.066
TRUST1	.081	-.108	.307	-.238	.652
TRUST2	.166	-.007	.132	-.109	.764
TRUST3	.260	.042	.066	-.138	.703
TRUST4	.168	.066	.200	-.192	.600
TRUST5	.136	-.011	.235	-.219	.662
PERF1	.679	-.098	.129	-.120	.191
PERF2	.693	-.031	.214	-.107	.306
PERF3	.641	-.023	.136	-.278	.199
PERF4	.633	-.177	.277	-.224	.079
PERF5	.717	-.097	.082	-.096	.098

Values $> .60$ represent primary loading. The negative loading of TECH is caused by the way it is oriented on the graphs, which is a direction artifact and is not a substantive finding; however, all of the TECH items load together without problems and the interpretation of the construct is not affected.

- **KMO and Bartlett's Test** Before running an EFA, it is important to establish that adequate sampling was obtained ($KMO > 0.60$) and that there is meaningful correlation among the items (Bartlett's Test, $p < 0.05$).

Table 3b: KMO and Bartlett's Test Summary

Measure	Value
KMO (Sampling Adequacy)	.858
Bartlett's χ^2	1658.48
df	300
Sig. (p)	<.001
Cumulative Variance Explained	60.00%

Result: $KMO = .858$, Bartlett's $\chi^2 = 1658.48$ ($p < .001$) — both confirm suitability for factor analysis. A five factor solution was obtained that accounted for 60.00% of the total variance and all items loaded above .60 (in magnitude) on their intended factor and there was little cross loading, which supports construct validity.

4.5 Descriptive and Correlational Statistics

Each of the constructs is reported with descriptive statistics that describe the central tendency (mean) and spread (SD). As a preliminary check before the regression, Pearson correlation is used to measure the strength and direction of linear relationship between the constructs.

Table 4: Descriptive Statistics

Construct	M	SD
TECH	3.876	.554
ORG	3.962	.610
ENV	3.750	.561
TRUST	3.826	.532
PERF	4.407	.485

Result: PERF scores highest and ENV lowest, suggesting respondents feel more confident about performance outcomes than about environmental/regulatory pressure driving adoption.

• Pearson Correlation

Pearson correlation coefficient quantifies the magnitude and direction of the linear relationship between two constructs, which will range from -1 to +1 with higher values closer to ± 1 signifying a stronger linear relationship between the constructs, and values closer to 0 signifying little or no linear relationship between the constructs. It is a preliminary description that was done in order to check whether or not there are variables that move together, without controlling other variables or with the assumption that these variables are causing one another.

Table 5: Pearson Correlation Matrix

	TECH	ORG	ENV	TRUST	PERF
TECH	1				
ORG	.313**	1			
ENV	.192*	.002	1		
TRUST	.462**	.456**	.040	1	
PERF	.458**	.426**	.192*	.515**	1

** $p < .01$, * $p < .05$ (two-tailed).

Result: The correlation of TRUST is the highest with PERF (.515), predicting its role in mediation. ENV is least correlated with ORG (.002) and TRUST (.040), and is distinct from the other constructs early on in the analysis.

4.6 Multiple Regression

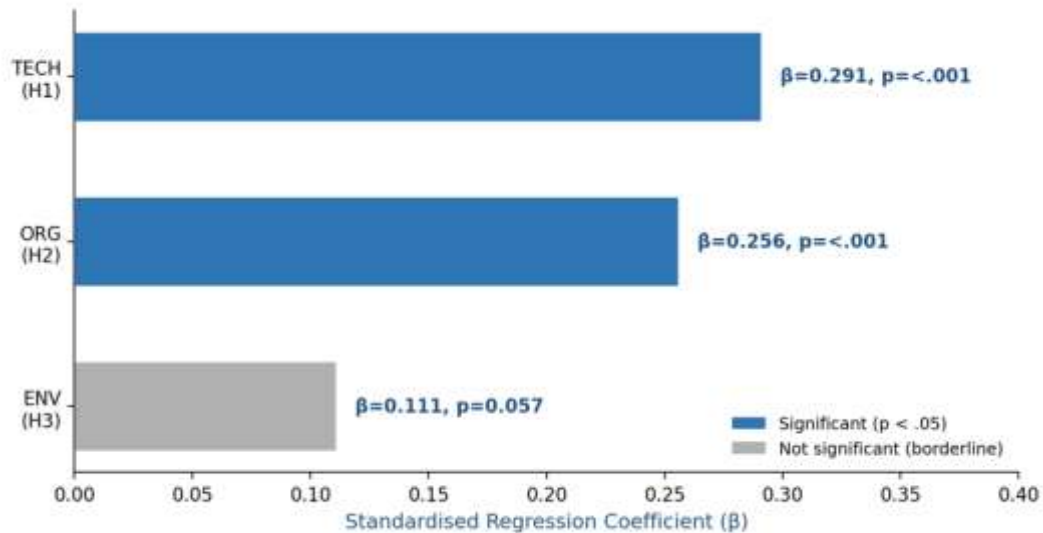
The multiple regression determines whether TECH, ORG and ENV significantly predict PERF when each other is controlled. Multicollinearity: VIF < 5 is acceptable. Autocorrelation: Durbin-Watson close to 2.0 is not a concern.

Table 6: Regression Results (DV: PERF)

Predictor	β	SE	t	p	VIF
TECH	.291	.062	4.721	<.001	1.155
ORG	.256	.055	4.654	<.001	1.113
ENV	.111	.058	1.916	.057	1.042

$R^2=.314$, Adj. $R^2=.301$, $F(3,160)=24.37$, $p<.001$, Durbin-Watson=1.998.

Result: Perception of effectiveness is significantly and positively predicted by TECH (H1 supported) and ORG (H2 supported). ENV's coefficient is positive but not significant (H3 is not supported at $p<.05$). Multicollinearity is not a likely cause since the VIF values are close to one.

**Figure 2: Regression Coefficients Predicting Adoption/Performance**

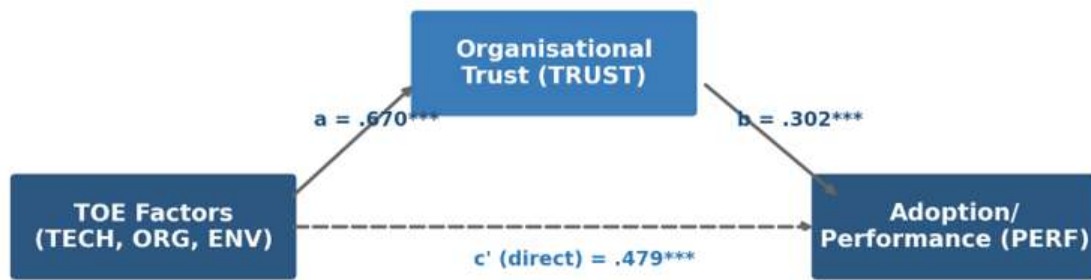
4.7 Mediation Analysis

Hayes' PROCESS Model 4 breaks the overall TOE→PERF effect into a direct effect and an indirect effect that goes through TRUST. A bootstrap confidence interval (5,000 resamples) does not include zero, indicating that there is significant mediation, but if the direct effect is significant, then there is partial mediation, not full.

Table 7: Mediation Path Results

Path	Coefficient	p	95% CI
TOE → TRUST (a)	.670	<.001	[.482, .858]
TRUST → PERF (b)	.302	<.001	[.174, .430]
TOE → PERF, direct (c')	.479	<.001	[.301, .657]
Indirect effect ($a \times b$)	.202	—	[.116, .304]

Result: Both paths are important and the indirect path is not in the null zone, indicating mediation. The direct effect still is very prominent, suggesting partial rather than full mediation (H4 supported).



Indirect effect ($a \times b$) = .202, 95% CI [.116, .304] — Partial Mediation Confirmed

Figure 3: Mediation Model — TOE → Trust → Performance

4.8 Hypothesis Summary

Table 8: Hypothesis Summary

Hypothesis	Path	Decision
H1	TECH → PERF	Accepted
H2	ORG → PERF	Accepted
H3	ENV → PERF	Rejected (borderline)
H4	TOE → TRUST → PERF	Accepted (partial mediation)

4.9 Secondary Data Analysis

This sub-section (4.10) provides an analysis of secondary data – company disclosure and financial performance – to serve as a triangulation layer to the findings from the primary data outlined above for the ten sampled organisations.

4.10 Secondary Data: Disclosure and Financial Triangulation

Since 10 companies are not enough to conduct reliable inferential testing, the ADCI disclosure scores of all ten sampled companies were analysed descriptively along with the financial performance of the companies (Net Profit and ROA) in FY 2024-25. The results in this section answer RQ3 – they suggest that while the individual-level perceptions of adoption do not track the sub-sector regulatory intensity, the more formal disclosures of companies do. This tracking of regulatory intensity seems to be a robust pattern – despite the only marginal significance of Environmental Pressure in the primary regression in Section 4.5, the companies with the highest scores on ADCI (private banks) and the lowest scores (NBFCs and the insurer) follow this pattern. The results in this section are the most distinctive of the study, and suggest that the same regulatory pressure is registered at the institutional level compared to the individual level.

Table 9: ADCI Scores and Financial Performance (FY 2024-25)

Company	ADCI (/20)	Net Profit (₹ Cr)	ROA (%)
ICICI Bank	10	47,227.00	2.23
Axis Bank	10	26,373.48	1.59
Bajaj Finserv	9	8,872.31	1.65
HDFC Bank	9	67,347.40	1.72
State Bank of India	8	70,901.00	1.07
Bajaj Finance	8	16,779.00	3.61
Shriram Finance	6	9,761.00	3.32
HDFC Life	3	2,461.00	0.73
Kotak Mahindra Bank	2	16,450.00	1.87

Company	ADCI (/20)	Net Profit (₹ Cr)	ROA (%)
Jio Financial Services	1	1,612.59	1.11

Sample mean ADCI = 6.6/20. Kotak Mahindra Bank's score carries lower confidence due to limited source-document accessibility during coding.

Result: Private banks cluster at the top (9–10/20); NBFCs and the insurer cluster lower (1–6/20) — evidence that regulatory exposure shapes disclosure behaviour even where the individual-level ENV effect in the survey was only marginal.

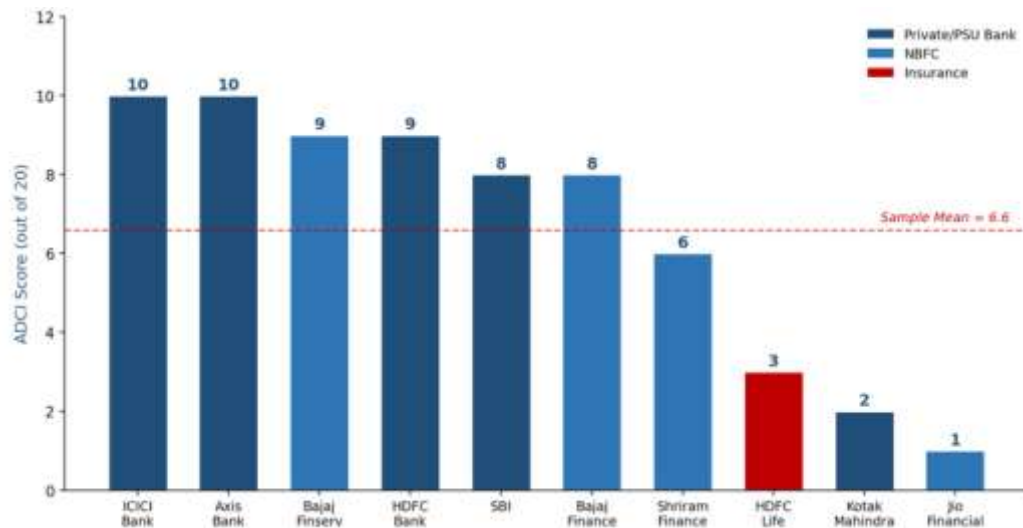


Figure 4: AI-Driven Cybersecurity Disclosure Intensity (ADCI) by Company

5. Discussion and Conclusion

5.1 Discussion

TECH and ORG emerged as the strongest predictors of performance outcomes attributable to AI-driven cybersecurity adoption (PERF), supporting Arroyabe et al. (2024), who similarly found internal digital capability outweighing external pressure among European SMEs. This pattern also aligns with Badghish and Soomro (2024), who identified compatibility and organisational readiness — rather than environmental mandate — as the dominant AI-adoption drivers. Unlike Sánchez et al. (2025), however, who found cybersecurity concern operating as a significant environmental barrier, this study's ENV effect was only borderline at the individual level — a divergence plausibly explained by this study's secondary-data finding that regulatory pressure operates more forcefully at the institutional-disclosure level than the individual-perception level, a distinction Sánchez et al.'s single-source design could not have detected. HDFC Life's low ADCI score despite an actual, disclosed 2024 breach further indicates disclosure maturity and incident exposure are not intrinsically linked. This study applied the trust-in-technology framework by McKnight et al., (2002) in the AI-cybersecurity context to test the framework statistically for the first time in this domain, even though the framework had been theorised in the field of AI-cybersecurity.

5.2 Theoretical Contribution

This study has three important theoretical implications. First, it extends the framework of the TOE, which has already been validated, most prominently in the general context of enterprise AI adoption (Arroyabe et al., 2024; Badghish & Soomro, 2024; Sánchez et al., 2025), to one specific context: AI for cybersecurity. It is important to note that the same three dimensions found in the TOE in the general context of enterprise AI adoption are found in the specific context of AI for cybersecurity. Second, it introduces Trust theory (Mayer et al., 1995; McKnight et al., 2002) as a mediation mechanism into the TOE model, rather than the trust being a peripheral or unmeasured background condition, it can be shown to empirically mediate the TOE effect and statistically transmit a part of the effect on the TOE on to the performance measure. Third, and most importantly, the study shows for the first time through its triangulated design that the relationship between two different levels of the same theoretical construct (ENV – at the institutional level, and at the individual level) can be different; ENV had only a borderline effect in the individual perception data, but a patterned effect in the company-level disclosure behaviour. The current study is the first to document this discrepancy in the TOE literature, where nearly all analyses have used single-source data, and implies that future TOE-based research should be careful not to take perceptual and archival measures of the same construct as equivalent.

5.3 Practical Implications

5.3.1 Implications for Managers

Deliberate capacity building, backed by management support, sufficient investment and employee training, is most effective when paired with AI-based cybersecurity investments for optimal returns, not technology

investments alone. Since Trust is a partial mediator of the TOE – Performance relationship, the steps towards building trust should be considered a separate workstream from the technical deployment of the AI solution – otherwise managers may assume that simply having an AI solution in place leads to trust.

5.3.2 Implications for Policymakers

The institutional-level pressure is less than the individual-level pressure, indicating that even though the latter may not yet be fully embedded in the awareness of individual employees, formal disclosure pressures like BRSR are nevertheless influencing what is reported. This means disclosure regulation is not enough to create a real culture of AI-cybersecurity readiness at the employee level and should be complemented with other, related, internal culture change needs.

5.3.3 Implications for Researchers

The fact that there is an apparent difference between individual-perception and institutional-disclosure measures of environmental pressure indicates that future TOE-based studies should not assume that measures at the individual level generalise across levels. The sub-sector stratification of the ADCI scores (banks disclosing significantly more compared to NBFCs and insurers) also serves as a reference point for future disclosure research on similar comparative or longitudinal studies.

5.4 Limitations

- **Sample composition:** Market-cap ranking skews the sample toward banking/NBFC, with minimal insurance and no asset-management representation — limiting generalisability beyond this sub-set.
- **Total Assets verification:** Only 4 of 30 firm-year figures are confirmed on a standalone basis; the remainder await further verification.
- **ADCI confidence:** Scores vary in reliability by firm depending on source-document accessibility; Kotak Mahindra Bank's score reflects limited material, not confirmed low disclosure.
- **Common-method bias:** A standard concern for single-source, self-report data; not directly tested via Harman's single-factor procedure in this iteration.
- **Cross-sectional design:** Primary data reflect a single point in time; causal claims should be treated as provisional pending longitudinal validation.

5.5 Conclusion

The aim of this study was to explore the influence of Technological, Organisational and Environmental factors on both adoption and their performance effect on AI-based cyber security solutions and to identify the role of organisational trust in the relationship between the two. The studies show that the interaction of technological readiness and organisational capacity is a significant influence on the outcomes of its usage in cyber security, with both factors having robust and statistically significant effects on the outcomes realized. The impact of environmental pressure was more subtle: just at the level of individual perception, and clearly at the institutional-disclosure level, as higher-disclosing banks have a distinct profile from lower-disclosing NBFCs and insurers. Organisational trust was identified as a partial mediating mechanism, as some of the positive impact of high technological and organisational levels goes through the level of trust the employees have in these systems. The combination of these findings suggest that the adoption of AI for cybersecurity is not just a technical implementation, but a socio-technical process where organisational readiness and trust-building play a crucial role alongside the technology itself. The triangulated approach taken in this research, which combines primary perceptual data with independently verified secondary disclosure data from an identical organisational sample, provides a replicable template for future research to test the extent to which what organisations say internally matches what they formally disclose externally – a critical question with increasing relevance as AI governance disclosure requirements expand globally.

References

1. Arroyabe, M. F., Arranz, C. F. A., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Analyzing AI adoption in European SMEs: A study of digital capabilities, innovation, and external environment. *Technology in Society*, 79, 102733. <https://doi.org/10.1016/j.techsoc.2024.102733>
2. Badghish, S., & Soomro, Y. A. (2024). Artificial intelligence adoption by SMEs to achieve sustainable business performance: Application of technology-organization-environment framework. *Sustainability*, 16(5), 1864. <https://doi.org/10.3390/su16051864>
3. KPMG. (2025). *Cybersecurity considerations 2025: Financial services sector*. KPMG International.
4. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. <https://doi.org/10.5465/amr.1995.9508080335>
5. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
6. Nadella, G. S., Gonaygunta, H., Kumar, D., & Pawar, P. P. (2024). Exploring the impact of AI-driven solutions on cybersecurity adoption in small and medium enterprises. *World Journal of Advanced Research and Reviews*, 22(1), 1190–1197. <https://doi.org/10.30574/wjarr.2024.22.1.1185>
7. Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, 14(1), 110–121.

8. Ponemon Institute. (2024). The 2024 study on the state of AI in cybersecurity. Ponemon Institute LLC.
9. Sánchez, E., Calderón, R., & Herrera, F. (2025). Artificial intelligence adoption in SMEs: Survey based on TOE–DOI framework, primary methodology and challenges. *Applied Sciences*, 15(12), 6465. <https://doi.org/10.3390/app15126465>
10. Tornatzky, L. G., & Fleischer, M. (1990). *The Processes of Technological Innovation*. Lexington Books.