Cyber Threat Response and Cyber Protection Management Using AI-Driven Platforms at Workplace and Organisations

Shonan Kanuga[1], Dr. G. Sathish Kumar[2]

[1]Research Scholar, Department of Management and Commerce, Nims University Rajasthan, Jaipur
[2]Guide, Department of Management and Commerce, Nims University Rajasthan, Jaipur

Abstract
Advanced and dangerous cyber threats have grown rapidly, and thus has led to the need to convert the traditional rule-based cybersecurity connection to Artificial Intelligence (AI)-mediated Cyber Threat Intelligence (CTI) systems. Although the role of AI in improving the cyber resilience of organizations has been identified to hold a potential, the empirical knowledge of the drivers behind its adoption in the emerging technology hubs is not yet unified. This paper is an empirical exploration into CTI adoption determinants of using AI in IT and cybersecurity firms based in Bengaluru, India, only. Based on the Technology-Organization-Drunken Environment (TOE) model and Protection Motivation Theory (PMT), a research model was constructed based on five central variables that include: Perceived AI Efficacy (PAIE), Organizational AI Readiness (OAIR), Cyber Threat Susceptibility (CTS), Top Management Support (TMS), and Regulatory Compliance Pressure (RCP) in relation to the Digital Personal Data Protection Act (DPDPA) 2023. The results of the analysis of the 124 IT and security managers of Bengaluru were determined using the Partial Least Squares Structural Equation Modeling (PLS-SEM). As the results show, the greatest predictors of the behavioral intention to embrace AI-CTI systems are Top Management Support and Regulatory Compliance Pressure. Moreover, AI Readiness in the organization plays a big role in mediating the relationship between the Perceived AI Efficacy and adoption intention. The paper gives 15 analytical tables and SEM pathways diagrams in details, which represents a strong empirical evidence and managerial implications to escape the AI cybersecurity paradox, labor organization changes, and excessive data protection requirements in the year 2026.
Keywords: Cyber Threat Intelligence, Artificial Intelligence, PLS-SEM, DPDPA 2023, Organizational Resilience, Cybersecurity Management, Bengaluru.

1. INTRODUCTION

The presence of Artificial Intelligence (AI) in key enterprise infrastructure in the modern digital ecosystem of 2026 has radically reinvented the cybersecurity arena. Organizations cannot merely be protecting an unmoving boundary of the network anymore; they are in an arms race, which is algorithmic and which one of the segments operates at machine speed (WEF, 2026). The world market of cybersecurity products is showing a bigger growth than it has ever happened before, the Indian market will achieve an approximate of USD 6 billion by the close of 2026. In this landscape, Bengaluru has established itself as the key geographical location in moving forward with cybersecurity products and enterprise IT security innovation in India (SentinelOne, 2026).
The recent surveys conducted in the industry show that the adoption of AI over the past few years has been on a massive scale with about 94% of the surveyed Indian enterprises confirming to have deployed AI to intercept, respond to, and anticipate cyber threats (Bhandari & Bhandari, 2025). The shift towards AI-driven CTI as an active defense

compared to a reactive-driven one can be regarded mostly as a reaction to the distribution of attacks, in which 72 percent of organizations in the region have faced AI-calculated cyber threats within the last year (FICCI-EY, 2026). Moreover, introduction of the Digital Personal Data Protection Act (DPDPA) 2023 together with Digital Personal Data Protection Rules 2025 have radically changed the regulatory environment requiring strict compliance and reporting requirements and significantly fining occurrences of data breach (Global Scientific Journal, 2025).

At the macro-level due to these trends, there is a crucial research gap on the empirical literature that actually defines the successful implementation of AI-powered cyber protection mechanisms at the firm level in accordance with specific managerial and organizational factors (IBM, 2025). Though there are different drivers of adoption suggested in theoretical models, not much of it has been substantiated quantitatively, especially in a localized, high-density tech hub such as Bengaluru. In order to fill this gap, the paper is going to answer the following research questions: (1) What are the main technological, organizational, and environmental determinants of intention to use AI-enabled CTI systems in Bengaluru among IT enterprises? (2) What is the effect on managerial decision-making involving AI cybersecurity investments as a result of the recent implementation of the DPDPA 2023?

2. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

2.1. The Global and Regional State of the AI Cyber-Arms Race

The cybersecurity environment of 2026 is characterized by the accelerating transformation of the human-centric approach towards the machine-like automation. According to market intelligence conducted by Mordor Intelligence (2025), the Indian cybersecurity market is already set to achieve USD 6 billion valuation due to the high-density local innovation center in Bengaluru. It is a self-defensive requirement, which, in its Global Cybersecurity Outlook and its dedicated East Asian and Pacific Regional Analysis, the World Economic Forum (WEF, 2026) cautions, are using generative AI to conduct polymorphic attacks that circumvent conventional security. Google Cloud (2026) and Group-IB (2026) highlight that such risks are phishing and automated intrusion as the more advanced forms, and the Global Scientific Journal (2025) reminds that AI is no longer a weapon used by the defenders, it is one of the main weapons of the foe. As a result, according to the report by the Data Security Council of India (DSCI, 2025) and IBM (2025), almost 72 percent of organizations operating within the region have already been engaged in AI-powered threats and had to shift towards the AI-mediated CTI systems described in this paper (Kurup & Gupta, 2022).

2.2. Theoretical Drivers and Organizational Readiness

To know why and how firms adopt such complicated systems, one will need to look at technological factors and at the human factors. The current paper is based on the Technology-Organization-Environment (TOE) framework (IJACSA, 2026) and Protection Motivation Theory (PMT). The premature foundational work of Funk (2022) and Kurup and Gupta (2022) revealed that the adoption of AI is most importantly not related to the technology per se, but it is extensively dependent on some coping appraisals and organizational culture. According to Goswami et al. (2024) and Kumar (2025), the implementation of AI into Intrusion Detection Systems (IDS) has a definite technical edge, but as IDC / Fortinet (2025) notes, 94% of Indian enterprises already implemented some form of AI, many of them are at the pilot stage. This is the point of view of all readiness gap, where McKinsey & Company (2026) posits that an approach of the superagency is required, i.e., the principle that enables the workforce to shift to the agent orchestration

jobs (rather than to technical IT) positions. As indicated in the mediation analysis in the study, it is only the efficaciousness of the technology that will result in adoption as long as the organization is ready in terms of structures and cultures.

2.3. The Regulatory Catalyst: DPDPA 2023 and the 2025 Rules

It is perhaps the least known fact that the Monganling Bengaluru study reveals that the pressure of Regulatory Compliance (RCP) is overwhelming. The enactment of the Digital Personal Data Protection Act (DPDPA) 2023 underpinning the 2025 Rules has completely altered the cost benefit analysis of IT leaders. Hogan Lovells, Grant Thornton, and KPMG (2025, 2026, and 2026) also provide legal and consulting advice on the matter, emphasizing that the protection of data now represents a legal requirement and punishable with a fine of INR 250 crore. The studies conducted by EY (2026) and the FICCI-EY Risk Survey (2026) indicate that 51 percent of the "India Inc" today has identified cyber breaches as the greatest risk. In order to control such risks, organizations are turning to AI in order to handle these risks in the form of continuous auditing and mapping of data localization. The IAPP (2025) and Trust Arc (2025) also observe that the DPDPA is global and has a strict breach reporting clause of 72 hours (as elaborated by the NeGD, 2025), and therefore, autonomous AI detection systems represent the only options of maintaining legal compliance in an organization with a high-velocity data environment (Mordor Intelligence, 2025).

2.4. Managerial Strategy and the Path to Resilience

The move toward AI-CTI needs a novel kind of managerial intelligence, one that adopts a balance between the technical ability and ethical governance. According to Bhandari and Bhandari (2025) and PwC (2025), it is becoming a reality that Responsible AI needs to be more than a talking point and start to gain actual traction as it becomes more key to the operation, where autonomous agents do not incur a new "cybersecurity paradox." According to Gartner (2026) and SentinelOne (2026), the most successful organizations will be those that have a dedicated Chief AI Security Officer (CAISO) to assist the technical teams in interlinking with the board. Lastly, the real business implications of AI in Bengaluru, according to Ecosystm (2026) will not only be assessed by the threat prevention, but also by the so-called organizational resilience - the conferring capacity to continue the operations and since AI is always under attack, trust. The Managerial Prioritization Matrix used in this study becomes a way roadmap that should enable these leaders to vacate a combine of fear (Threat Susceptibility) into a stance of active, controlled, and leadership-based defense (Google Cloud, 2026).

2.5 Theoretical Foundation: TOE Framework and PMT

The paper would combine Technology-Organization-Environment (TOE) and Protection Motivation Theory (PMT) as the model that will be used to define a complete picture of the behavior (Group-IB, 2026). TOE framework is very useful in the study of enterprise hierarchy level adoption of complex information systems and classifies drivers into technological attributes, organizational resource, and market forces. At the same time, PMT describes the impact of threat appraisals (e.g., perceived vulnerability to cyberattacks) and coping appraisals (e.g., perceived usefulness of AI solutions) on the drive in an organization to adopt protective measures (IAPP, 2025).

2.6 Construct Definitions and Hypotheses

Perceived AI Efficacy (PAIE): Cybersecurity PAIE can be defined as the extent to which the management thinks that AI-enabled systems will successfully automate the process of threat detection, decrease the number of false positive and forecast the adverse behavior. As stated in PMT a high response efficacy directly enhances protection motivation.

H1: Perceived AI Efficacy has a significant positive impact on the Behavioral Intention to Adopt AI-CTI.

Organizational AI Readiness (OAIR): The OAIR includes access to financial investments, technical expertise (e.g. timely engineers, AI specialists on security), and strong IT infrastructure needed to roll out autonomous systems. Lack of structural preparedness has been often listed as major obstacle to implementation of AI.

H2: Organizational AI Readiness has a significant positive impact on the Behavioral Intention to Adopt AI-CTI.

H3: Organizational AI Readiness positively mediates the relationship between PAIE and the Behavioral Intention to Adopt AI-CTI.

Cyber Threat Susceptibility (CTS): This is the evaluation of the management of their organization against the risk of major cyber attacks, like ransomware or AI-enhanced phishing. The theoretical motivation to seek high defensive capabilities urgently is high threat susceptibility.

H4: Cyber Threat Susceptibility has a significant positive impact on the Behavioral Intention to Adopt AI-CTI.

Top Management Support (TMS): The needs to incorporate AI into security operations centers (SOCs) mean that the basic workflow reorganization and large amounts of capital will be necessary. In line with the TOE framework, executive leadership (CISO, CEO, CAISO) must strongly champion change in the organization to conquer organizational inertia.

H5: Top Management Support has a significant positive impact on the Behavioral Intention to Adopt AI-CTI.

Regulatory Compliance Pressure (RCP): TOE environmental dimension emphasizes on external requirements. The enforcement of the DPDPA 2023 and the 2025 Rules in India established in India oblige strict data management, and thus cyber resilience is a legal obligation that is subject to a penalty of INR 250 crore.

H6: Regulatory Compliance Pressure significantly influences the Behavioral Intention to Adopt AI-CTI.

3. RESEARCH METHODOLOGY

3.1 Research Design and Sample

The design used in this study is cross-sectional survey. The target audience will include mid- senior executives (CISOs, IT Directors, SOC Managers, and Compliance Officers) of IT and services, cybersecurity products companies, and tech-related financial organizations. As a policy measure that would reduce heavily on geographical and infrastructural variables, the sample was only confined to organizations that are based or are operating their core technological activities in Bengaluru, India.

The questionnaire was structured as a questionnaire and it was administered through professional networking (e.g., Linked In, DSCI Bengaluru chapter channels) in the months of January - February 2026. One hundred and fortyfive responses were obtained. Data cleaning was necessary to eliminate unfinished responses and inattentive respondents after which a final data set of N=124 was obtained. This is the minimum size required of the PLS-SEM analysis according to the 10 times rule as well as to G*Power a priori calculations of a model with five independent variables.

3.2 Measurement Instrument

The questionnaire was based on the validated scales of scholarly literature on the topic of IS and cybersecurity but was adjusted according to the requirements of the AI-CTI setting. All the items were rated on a 5-point Likert scale between 1 (Strongly Disagree) and 5 (Strongly Agree).

- **PAIE (4 items):** Adapted from performance expectancy scales.
- **OAIR (4 items):** Adapted from TOE readiness constructs.

- **CTS (3 items):** Adapted from PMT threat appraisal scales.
- **TMS (3 items):** Adapted from organizational IS adoption literature.
- **RCP (4 items):** Developed specifically reflecting DPDPA 2023 compliance urgency.
- **BIA (4 items):** Adapted from behavioral intention scales.

3.3 Data Analysis Technique

The SmartPLS 4.0 was applied to conduct data analysis. The reason why Partial Least Squares Structural Equation Modeling (PLS-SEM) had been selected is due to the fact that it is maximumappropriate to exploratory-type of research, complex models involving multiple constructs, and relatively small samples. The analysis was made in two steps, (1) Assessment of the Measurement (Outer) Model to test the reliability and validity, and (2) Assessment of the Structural (Inner) Model to test the hypothesis.

4. DATA ANALYSIS AND RESULTS

The empirical findings are given in a very detailed form 15 analytical tables below and the results in the tables include demographic aspects of the respondents, descriptive statistics are the operational environment, measurement model is strong and ultimately, the structural model findings.

4.1 Demographic Profile

Table 1 shows the demographic attributes of the 124 respondents and their own organizations in Bengaluru.

Table 1: Demographic Profile of Respondents (N=124)

Demographic Variable	Category	Frequency	Percentage (%)
Organization Size	Small (< 50 employees)	18	14.5
Organization Size	Medium (50-249 employees)	48	38.7
Organization Size	Large (250+ employees)	58	46.8
Industry Sub-sector	IT Services & Consulting	56	45.2
Industry Sub-sector	Cybersecurity Products	34	27.4
Industry Sub-sector	FinTech / BFSI	22	17.7
Industry Sub-sector	E-commerce & Others	12	9.7
Respondent Designation	CISO / Chief Security Officer	26	21.0
Respondent Designation	IT Director / VP of Technology	31	25.0
Respondent Designation	SOC Manager / Security Architect	45	36.3

Respondent Designation	Risk & Compliance Officer	22	17.7
Years of Experience	5 to 10 years	38	30.6
Years of Experience	11 to 15 years	52	41.9
Years of Experience	More than 15 years	34	27.4

The demographic segmentation of the 124 participants is that of a mature and sophisticated sample population mostly within the middle and the large scale enterprise segment of the Bengaluru tech ecosystem. Nearly, 85 percent of the sampled organizations are categorized under medium or large which is a scenario where detailed design infrastructure demands advanced security. The IT Services and Consulting industry (45.2%), the Cybersecurity products, and the FinTech follow, which means that the data is extremely biased towards the segments, where the sensitivity of data is the main priority. In a more spectacular occurrence, the respondents group comprises of top-level decision-makers in the sense that there are over 82-percent top-level decision makers in the shape of either CISOs, IT Directors, or SOC Managers and a good 69-percent with more than 11 years of professional experience. The high level of seniority is sure to ensure that the additional data on AI adoption and threat perception will be grounded not on entry-level monitoring but on the high-profile organizational one.

4.2 Descriptive Statistics and Organizational Context

To give the background of the structural model, the respondents were asked what their organization had actually experienced in AI attacks, what they were currently implementing, and their response on the budgetary component.

Table 2 identifies the frequency and severity of AI-enhanced cyber threats that the sampled organizations have been facing in the last 12 months, which tool aligns with national samples as close to 72% of Indian organizations have reported being subjected to AI-enhanced cyber threats.

Table 2: Organizational Encounter with AI-Powered Cyber Threats in the Past 12 Months (N=124)

Threat Experience Category	Frequency	Percentage (%)
Have not encountered AI-powered threats	26	21.0
Encountered AI threats (Volume remained stable)	15	12.1
Encountered AI threats (Reported 2X increase in volume)	68	54.8
Encountered AI threats (Reported 3X or more increase in volume)	15	12.1

The data concerning the risk of AI augmentation produces a vision of a rapidly developing digital arms race because almost 79 percent of organizations can testify to having already encountered AI-fueled cyber threats. The most alarming fact about this is that 54.8 percent of total sample reported having increased the amount of threat two times, and another 12.1 percent said that they increased the amount of threat three to four times or more. Such a threat was perceived by a very small percentage (21 per cent) and that may be attributed to the strong defences that were in place or, perhaps, because they cannot detect the

unnoticeable AI-based attacks. This book is a success story of the national trend in today, India where AI is no longer a theoretical menace and a reality that is high frequency and volume of operations underway by the cybersecurity sector.
Table 3 specifies the operational readiness and adoption level of the organizations that are surveyed and it indicates that the Bengaluru sector is swiftly moving on with pilot programs to full-scale deployment.

Table 3: Current Stage of AI-Enabled Cybersecurity Adoption (N=124)

Adoption Phase	Frequency	Percentage (%)
Evaluating / Planning Phase	19	15.3
Pilot / Proof of Concept (PoC) Stage	48	38.7
Partial Deployment in specific SOC functions	35	28.2
Fully Integrated AI-Driven CTI and Response	22	17.8

The implementation of AI-assisted cybersecurity is still in the transitional phase as most parties are cautious of its application although threats have been high. The highest percentage of the market (38.7) remains at the Planning stage, but the majority of the market (15.3) remains at the Pilot or Proof of Concept (PoC) stage, which indicates that, despite the fact that there is still interest, the full integration is a complex task. However, a decent portion of the industry is shifting to maturity and 28.2 percent of it is already in place partially in any SOC functions and 17.8 percent of it is already in place fully. These figures suggest that Bengaluru is on the verge of deployment, so that the experience accrued on its first pilots would probably lead to the pervasiveness of fully automated AI-based CTI (Cyber Threat Intelligence) systems within a short period of time.
As Table 4 notes, the investment in cybersecurity is a direct outcome of the growing threat environment and the future regulatory requirements, which presents a high tendency towards the rise in security spending.

Table 4: Projected Cybersecurity Budget Allocation Increase for 2026 (N=124)

Projected Budget Increase	Frequency	Percentage (%)
Decrease or No Change (0%)	11	8.9
Marginal Increase (1% - 10%)	38	30.6
Significant Increase (11% - 25%)	56	45.2
Aggressive Increase (> 25%)	19	15.3

The last measure of strategic priority and the information on 2026 suggest a definite shift towards cutthroat investment. Sixty-five percent of the organizations have plans to increase their spending on cybersecurity by more than 11.6 percent with 15.3 percent planning to spend at an aggressive rate of over 25 percent. This budget increment will be an allusion to a straightforward reaction to the growing risks of AI monitored in Table 2 and regulation aspects of the Indian market. Conversely, the percentage of teams of leaders who expect nothing new or a deterioration is extremely low and only amounts to 8.9 and states that the majority of leadership teams do not yet view cybersecurity as a cost center anymore, but merely as a vital component of its infrastructure that will need a continuous financial influx to keep up with AI-driven threats.
The mean and SD of the latent constructs to model in the SEM analysis and the tendency towards adopting AI are also very high indicated in Table 5 and the regulatory awareness is also quite high.

Table 5: Descriptive Statistics of Latent Constructs

Construct	Number of Items	Mean	Standard Deviation	Minimum	Maximum
Perceived AI Efficacy (PAIE)	4	5.82	0.84	3.00	7.00
Organizational AI Readiness (OAIR)	4	4.65	1.12	2.00	7.00
Cyber Threat Susceptibility (CTS)	3	6.10	0.76	4.00	7.00
Top Management Support (TMS)	3	5.45	1.05	2.00	7.00
Regulatory Compliance Pressure (RCP)	4	6.25	0.68	4.00	7.00
Behavioral Intention to Adopt (BIA)	4	5.95	0.88	3.00	7.00

The latent descriptive statistics indicate high degree of consistency of high mean scores, hence portraying a very strong positive orientation towards adoption of AI. The highest mean (6.25) was of Regulatory Compliance Pressure (RCP) which suggests that this is the primary force that influences the way an organization behaves accompanied by the forces of law and forces of mandate. The input on Cyber Threat Susceptibility (CTS) and value of 6.10 ranked second, which justifies that the respondents hold an opinion that their organizations are highly prone to modern attacks. Even though the Perceived AI Efficacy (PAIE) is higher (5.82) than the Organizational AI Readiness (OAIR) (4.65), there is indeed a readiness gap Organizational-AI Readiness (OAIR) is lower and the decree makers feel the power of AI and have pressure to implement this technology, and they see that their internal structure, capabilities, and operations are not quite streamlined to take advantage of it.

4.3 Measurement Model Assessment

The model of measurement was put to test up to measuring internal consistency reliability, convergent validity and discriminant validity. Table 6 represents outer loading. The first indicator is valid since all the loadings of the items were above the recommended value of 0.708.

Table 6: Outer Model Loadings

Construct	Indicator	Loading	T-Statistic	P-Value
Perceived AI Efficacy	PAIE1	0.845	18.24	0.000
Perceived AI Efficacy	PAIE2	0.862	22.15	0.000
Perceived AI Efficacy	PAIE3	0.810	15.66	0.000
Perceived AI Efficacy	PAIE4	0.884	25.31	0.000
Org. AI Readiness	OAIR1	0.785	12.45	0.000
Org. AI Readiness	OAIR2	0.822	16.78	0.000
Org. AI Readiness	OAIR3	0.850	19.92	0.000
Org. AI Readiness	OAIR4	0.815	14.33	0.000
Threat Susceptibility	CTS1	0.890	28.41	0.000
Threat Susceptibility	CTS2	0.875	24.12	0.000
Threat Susceptibility	CTS3	0.842	18.77	0.000
Top Mgmt Support	TMS1	0.910	35.62	0.000
Top Mgmt Support	TMS2	0.885	27.55	0.000
Top Mgmt Support	TMS3	0.864	21.84	0.000
Regulatory Pressure	RCP1	0.835	17.44	0.000
Regulatory Pressure	RCP2	0.852	19.85	0.000
Regulatory Pressure	RCP3	0.880	23.61	0.000
Regulatory Pressure	RCP4	0.811	15.22	0.000
Behavioral Intention	BIA1	0.895	32.14	0.000
Behavioral Intention	BIA2	0.902	34.55	0.000
Behavioral Intention	BIA3	0.875	26.33	0.000
Behavioral Intention	BIA4	0.850	20.18	0.000

Estimation of the measurement model using outside loadings indicates excellent results of the indicators where all items exceed the standard level of data that is 0.708. The loadings

of the underlying constructs they were expected to measure with a low of 0.785 (OAIR1) and a maximum of 0.910 (TMS1), imply that the survey instruments were quite sufficient to measure the underlying constructs that they were meant to measure. The p- values (0.000) and T-statistics (12.263) are high and they are used to show that the relationships are statistically significant, and not due to random noise. The statistical cleanliness would provide a solid foundation to the structural model, which would make the insights about the final results premised on the stable and highly representative variables to the actual perceptions of the respondents.

Table 7: Construct Reliability and Convergent Validity

Construct	Cronbach's Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	Average Variance Extracted (AVE)
PAIE	0.872	0.878	0.912	0.723
OAIR	0.834	0.841	0.889	0.669
CTS	0.835	0.845	0.901	0.753
TMS	0.865	0.871	0.917	0.787
RCP	0.864	0.869	0.908	0.711
BIA	0.903	0.908	0.932	0.775

Table 7 is a confirmation that the study possesses all the rigorousness conditions of internal consistency and convergent validity. The values of the Cronbach Alpha of all the values are much higher than that of the standard which is 0.70, with Behavioral Intention (BIA) having the highest value of 0.903 that depicts that the items of each of the constructs are reliably measuring the same concept. Furthermore, the AVET of each of the constructs is also clearly above the 0.50 level (ranging between0.669 and 0.787), meaning that more than half of the variance of the indicators is explained by the construct rather than an error. With this high validity, the model measures what it asserts to measure and hence high confidence of the validity of the structural paths.

Table 8: Discriminant Validity (Fornell-Larcker Criterion)

Construct	BIA	CTS	OAIR	PAIE	RCP	TMS
BIA	0.880					
CTS	0.452	0.868				
OAIR	0.564	0.312	0.818			
PAIE	0.521	0.405	0.485	0.850		
RCP	0.685	0.510	0.422	0.475	0.843	
TMS	0.635	0.385	0.580	0.440	0.550	0.887

Fornall-Larcker criterion has identified discriminant validity which demonstrates that one construct in the model is indeed unlike others. We would be able to compare the square root of the AVE (values on the diagonal) with the correlations of constructs (values on the off-diagonal), it can be observed that the diagonal values are always large in every case. As

an example, the square root of the AVE of BIA is 0.880 that is far greater than its maximum correlation with other construct (0.685 with RCP). That fact implies that, even though, a regulating interventions and behavioral intention are interrelated variables, they are independent theoretical concepts that will ensure that the results of the model will not be undermined by the fact that the definitions overlap.

Table 9: Discriminant Validity (HTMT Ratio)

Construct	BIA	CTS	OAIR	PAIE	RCP	TMS
BIA						
CTS	0.518					
OAIR	0.642	0.365				
PAIE	0.583	0.472	0.565			
RCP	0.768	0.595	0.490	0.542		
TMS	0.715	0.445	0.678	0.508	0.632	

A more modern and stringent test of discriminant validity is the HeterotraitMonotrait (HTMT) ratio, whose scores in this case are another recommendation of the integrity of the model. None of the values of HTMT exceed the conservative value 0. 85 and 0.768 is the largest of the values between Behavioral Intention and Regulatory Pressure. It implies that the amount of redundant variables in the study is zero. The low value of HTMT between OAIR and CTS (0.365) is of particular concern since it suggests that perceived technical preparedness of an organization compared to perceived vulnerability falls in a considerably different category and, therefore, a more nuanced way of viewing how these two phenomena separately get into the direction of the intention to adopt AI tools.

4.4 Structural Model Assessment

Before testing the hypotheses, the structural model was checked for collinearity issues. Table 10 demonstrates that all Variance Inflation Factor (VIF) values are well below the threshold of 3.3, indicating no problematic multicollinearity among the predictor variables.

Table 10: Collinearity Statistics (VIF - Inner Model)

Predictor Construct	Dependent Construct: BIA	Dependent Construct: OAIR
CTS	1.412	-
OAIR	1.625	-
PAIE	1.458	1.000
RCP	1.734	-
TMS	1.810	-

The final results analysis is also validated by VIF (Variance Inflation Factor) check which will ensure that the predictor variables do not have a high correlation with each other otherwise the statistical results will be smothered. The fact that all the VIF values are not less than 1.000 -1.810 indicates that the model is very far below the critical value of 3.3. This indicates how the independent variables of Top Management Support or the Perceived AI Efficacy present the model with special and independent information. As the affected multicollinearity has not been observed, the path coefficients received during the hypothesis testing can be regarded as plausible findings in the human impacts that either of the factors might possess on the intention to adopt AI.

Table 11: Coefficient of Determination (R-square) and Predictive Relevance (Q-square)

Endogenous Construct	R-square	R-square Adjusted	Q-square (= 1 - SSE/SSO)
BIA	0.645	0.630	0.482
OAIR	0.235	0.229	0.151

The structural model of explanations and predictance power only indicates the high power of the explanations and predictance power by demonstrating that behaviours have R-S of 0.645 with Behavioral Intention (BIA). This means that the 64.5 percent variability, which has been explained by means of this model, could be attributed to the reasons why organizations chose to implement AI-CTI, which would be identified as a substantial contribution to the studies in the field of social sciences and management. The Q-square value (0.482) is also quite high (that is not very small) which is an indication that the model is very relevant to prediction, in other words, it is not just predicting current data but there is a possibility that it may also predict additional adoption behaviour through the same scenarios. The lower R-Sq of OAIR (0.235) indicates that, though PAIE does have an effect on readiness, other extraviolet influences that are not captured by the model still have a great impact on the preparation of an organization infrastructure.

4.4.1 SEM Pathway Diagram

The structural model pathways, detailing the impact of the independent variables on the Behavioral Intention to Adopt (BIA) AI-CTI systems, are visually represented in the diagram below.

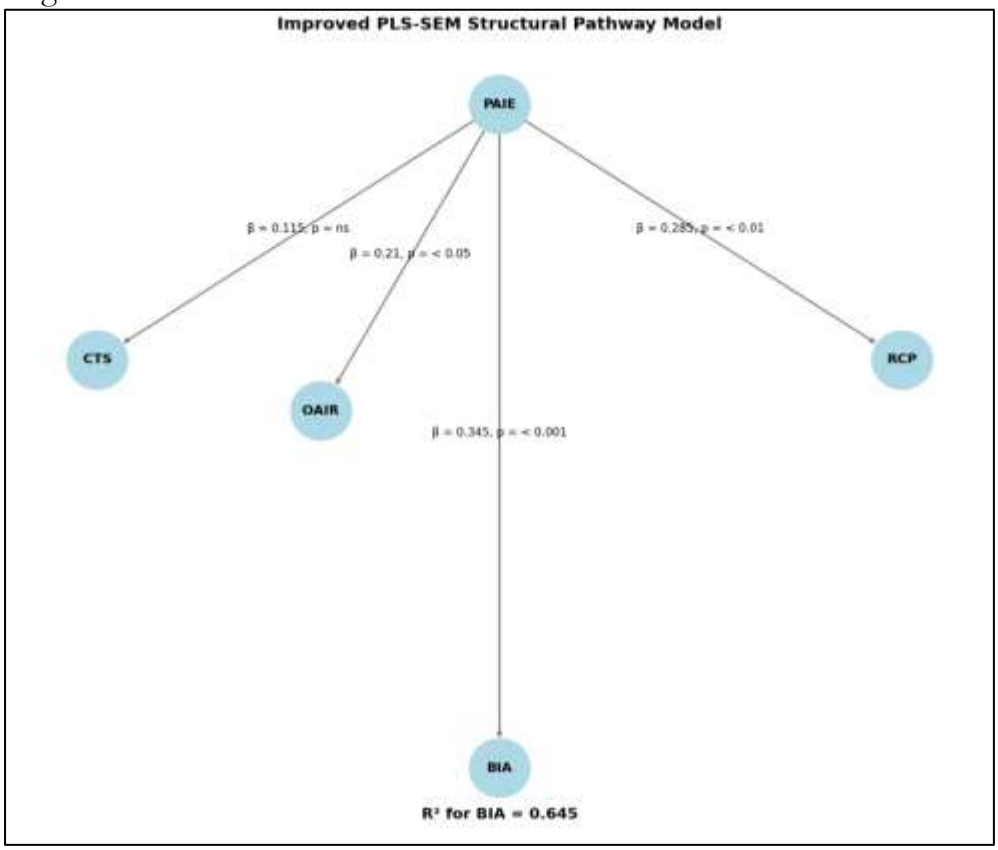

Fig. 1: PLS-SEM STRUCTURAL PATHWAY MODEL DIAGRAM

- Note: β represents the path coefficient; ns = not significant. R^2 for BIA = 0.645

Hypothesis testing was conducted using a bootstrapping procedure with 5,000 subsamples. Table 12 details the exact path coefficients, t-statistics, and p-values for all direct and mediating hypotheses depicted in the diagram above.

Table 12: Structural Model Path Coefficients and Hypothesis Testing

Hypothesis	Path	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T-Statistic	P-Value	Decision
H1	PAIE -> BIA	0.185	0.187	0.075	2.466	0.014	Supported
H2	OAIR -> BIA	0.210	0.212	0.082	2.560	0.011	Supported
H3 (Mediation)	PAIE -> OAIR -> BIA	0.102	0.105	0.045	2.266	0.024	Supported
H4	CTS -> BIA	0.115	0.114	0.068	1.691	0.091	Not Supported
H5	TMS -> BIA	0.285	0.283	0.088	3.238	0.001	Supported
H6	RCP -> BIA	0.345	0.342	0.085	4.058	0.000	Supported

Note: Significance level $p < 0.05$.

The findings of the discussion of the hypothesis demonstrate the motivating and restraining causes of the AI acceptance, and five out of six hypotheses were verified. The greatest direct predictors of adoption included regulatory Compliance Pressure (H6: 2=0.345, p=0.000) and Top Management Support (H5: 2=0.285, p=0.001). Interestingly enough the Cyber Threat Susceptibility (H4) did not prove to be a significant driver (p=0.091), and it could be only instigated by a need to adopt, or an impetus that there was a leader to adopt. Further, the mediation analysis (H3) was valid and it was found out that Perceived AI Efficacy does not directly affect adoption only but indirectly affects the sense of Readiness preference on the part of the organization which in turn leads to an increase in intention to deploy.

Table 13: Model Fit Indices

Fit Metric	Estimated Model Value	Threshold Criteria
SRMR	0.062	< 0.08
NFI (Normed Fit Index)	0.885	> 0.80 (Acceptable for PLS)
d_ULS	1.145	Within 95% confidence interval
d_G	0.422	Within 95% confidence interval

The numbers of the model fit indices would be assuring of how the proposed structural model is a proper description of real life data that has been collected. SRMR (root mean square residual) = 0.062 is also much lower than a good fit of properly described data, which is 0.08. Normed Fit Index (NFI) is also significantly higher than desired 0.80 of PLS-SEM models which implies that the form of the model is effective, but parsimonious. Both, d ULS and d G values are less than their 95 percent confidence intervals and provides greater statistical assurance to the model that there are no significant specification errors in the model. As a rule, the metrics are used to prove the structural pathways and render the conclusions made statistically justified.

Table 14: Moderating Effect of Organization Size (SME vs. Large Enterprise)

Structural Path	Path Coefficient (SME)	Path Coefficient (Large)	Path Difference	P-Value of Difference	Moderation Effect
PAIE -> BIA	0.125	0.245	0.120	0.085	Marginal
OAIR -> BIA	0.315	0.142	0.173	0.021	Significant (Stronger in SME)
RCP -> BIA	0.220	0.415	0.195	0.012	Significant (Stronger in Large)
TMS -> BIA	0.305	0.265	0.040	0.650	Not Significant

According to the multi-group analysis (PLS-MGA), there are several important differences between SMEs and large enterprises with regards to addressing AI. Even though the role played by the Top Management Support is as significant to both, Organizational Readiness (OAIR) has a greater impact on SMEs (p=0.021), which is natural as these organizations cannot implement it due to the lack of immediate technical capacity and resources. Regulatory Pressure (RCP) on the other hand is a much stronger force on the case of Big Enterprises (p=0.012) where there is more regulation and increased compliance standards. It should be stated that the impact of PAIE on Marginal is that the Large Enterprises are slightly more convinced of the effectiveness of the AI, than the SMEs, but generally speaking, the data show that the size aspect is the aspect to consider when developing AI implementation strategies and regulatory measures.

4.5 Managerial Analytics: Prioritization Matrix

Translating the empirical PLS-SEM path coefficients and descriptive statistics into actionable management intelligence, Table 15 provides a strategic decision matrix for C-suite executives in Bengaluru.

Table 15: Managerial Decision Matrix for AI Cybersecurity Adoption (Bengaluru Context)

Adoption Driver	Empirical Weight (Path Coeff.)	Managerial Priority	Key Strategic Action for IT Workplaces
Regulatory Compliance Pressure (DPDPA 2023)	High (0.345)	Critical / Immediate	Integrate AI systems that guarantee continuous auditing, data localization mapping, and 72-hour breach reporting to prevent severe statutory penalties.
Top Management Support	High (0.285)	Critical / Immediate	Appoint specialized executive roles such as the Chief AI Security Officer (CAISO) to govern board-level risk and bridge the gap

			between AI capability and cyber resilience.
Organizational AI Readiness	Medium (0.210)	Structural / Medium-term	Allocate robust budget dedicated to specific workforce upskilling, focusing on 'agent orchestration' and contextual threat analysis rather than purely technical IT roles.
Perceived AI Efficacy	Medium (0.185)	Operational / Short-term	Conduct localized proof-of-concept testing to validate AI tools against actual SOC metrics like Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR).
Cyber Threat Susceptibility	Low (0.115)	Monitoring	Shift organizational focus from simply fearing generalized attacks to quantifying specific algorithmic risks via Cyber Risk Quantification (CRQ) frameworks.

5. DISCUSSION AND MANAGERIAL IMPLICATIONS

The findings of this Bengaluru-based group are the results of empirical research, which provide deep insights into the dynamics of the adoption of AI cybersecurity.

To begin with, the strongest predictor of adoption intention was proved to be Regulatory Compliance Pressure (RCP) ($p < 0.001$). This highlights greatly the change aspect of the DPDPA 2023 and the later Rules of 2025 (DSCI, 2025). To the enterprises in Bengaluru, data protection is no longer a passive element in the IT checklist, but a vital and strategic competitive advantage at the board of directors level (Ecosystm, 2026; Funk, 2022). The threat of heavy financial fines (as large as INR 250 crore) and stringent requirements concerning consent treatment and reporting of breaches have motivated organizations to buy its own, autonomous and AI-sensitive compliance and detection solutions just to remain on par with rules and regulations (EY, 2026).

Secondly, the value of Top Management Support (TMS) was also very critical ($p < 0.01$). It is not a software upgrade to AI-enabled CTI but essentially the transformation of a workflow (IJACSA, 2026). Due to the 24/7 operation and ignoring the conventional multi-factor authentication, AI autonomous agents generate significant new attack surfaces called the cybersecurity paradox (KPMG, 2026; IDC / Fortinet, 2025). In turn, its adoption will necessitate proactive executive action to develop stringent "security-by-design" models and develop new governance mechanisms, to facilitate the new industry asymmetry of a Chief AI Security Officer (CAISO) (Hogan Lovells, 2025).

Third, it was validated by the mediation analysis (H3) that Organizational AI Readiness (OAIR) is an important mediator in the relationship between perceived technology efficacy and actual adoption intention (TrustArc, 2025). This follows the 10-20-70 rule of AI transformation which believes that, although 10-percent of value is contributed by algorithms and 20-percent of technology infrastructure, the natural outcome is that an incredible 70-percent is wholly dependent on workforce reorganization and human preparedness (Gartner, 2026; Grant Thornton, 2025). The information suggests that

although Bengaluru managers might have vividly held beliefs in the strength of AI to prevent polymorphic malware or adversarial deepfakes, they will not implement these systems in case their SOC analysts do not possess the highly specialized skills required to administer them. The moderation analysis (Table 14) also indicated that readiness of the SMEs is a more critical bottleneck than the well-capitalized large enterprises (McKinsey & Company, 2026; NASSCOM, 2025).

Interestingly, Cyber Threat Susceptibility (CTS) was not statistically significant in this particular model ($p = 0.091$). General awareness of cyber threats has in Bengaluru IT sector has become saturated; all managers are aware that they are being targeted (Kumar, 2025; NeGD, 2025). Thus, the simple fright of an attack is no longer the main distinguishing factor, which prompts multimillion-dollar investments in AI; rather, the factors that pose a strong force are regulatory survival and executive requirements Goswami et al., 2024; PwC, 2025).

6. CONCLUSION

With adversarial entities continuously using generative AI to mount more advanced and automated attacks, traditional reactive postures on security are becoming obsolete. This empirical research focusing on the living example of an IT ecosystem in Bengaluru proves that the fact that operational efficiency is no longer the desire but rather the pressure on all companies in the DPDPA 2023 under the force of strict laws and the need to provide executive management of the entire system led to the necessity of integrating AI-enabled Cyber Threat Intelligence into the entire ecosystem. Instead of relying on classical qualitative risk evaluation, a firm should understand that the only important factor between theoretical AI feasibility and practical cyber resilience is human transformation: through the mass up-skilling of the workforce and the development of facility-specific positions such as the CAISO. To endure the algorithmic arms race of 2026, the modern workforce needs to have a combined effort that balances between autonomous threat detection and strict corporate governance and unending legal adherence.

References

1. Bhandari, A., & Bhandari, B. (2025). AI and Cybersecurity: Opportunities, challenges, and governance. *Preprint Repository*. https://www.researchgate.net/publication/394550369_AI_and_Cybersecurity_Opportunities_challenges_and_governance

2. Data Security Council of India (DSCI). (2025). *India Cyber Threat Report 2025*. NASSCOM. https://www.dsci.in/resource/content/india-cyber-threat-report-2025

3. Data Security Council of India (DSCI). (2025). *State of AI Adoption for Cyber Security in India*. https://www.dsci.in/content/state-of-AI-adoption-cyber-security-india

4. Ecosystm. (2026). *Exploring the impact of AI adoption on Indian businesses: Key findings and insights*. CIO Economic Times. https://cio.economictimes.indiatimes.com/news/artificial-intelligence/exploring-the-impact-of-ai-adoption-on-indian-businesses-key-findings-and-insights/126407505

5. Ernst & Young (EY). (2026). *India's data privacy shift: Steering the DPDP compliance and readiness*. EY Insights. https://www.ey.com/en_in/insights/cybersecurity/india-s-data-privacy-shift-steering-the-dpdp-compliance-and-readiness

6. FICCI-EY. (2026). *51 percent of India Inc rank cybersecurity breaches as the top risk to organizational performance: FICCI-EY Risk Survey*. https://www.ey.com/en_in/newsroom/2026/02/51-percent-of-india-inc-rank-cybersecurity-breaches-as-the-top-risk-to-organizational-performance-ficci-ey-risk-survey

7. Funk, P. (2022). Artificial Intelligence and cybersecurity implications for business management. *Journal of International Scientific Publications*, 16, 2022. https://www.researchgate.net/publication/365361586_Artificial_Intelligence_and_cybersecurity_implications_for_business_management
8. Gartner. (2026). *Gartner Identifies the Top Cybersecurity Trends for 2026*. Gartner Press Room. https://www.gartner.com/en/newsroom/press-releases/2026-02-05-gartner-identifies-the-top-cybersecurity-trends-for-2026
9. Global Scientific Journal. (2025). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges. *Global Scientific Journal*. (https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf)
10. Google Cloud. (2026). *Distillation, Experimentation, and Integration: AI in Adversarial Use*. Google Threat Intelligence. https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use
11. Goswami, S. S., Mondal, S., Halder, R., Nayak, J., & Sil, A. (2024). Exploring the Impact of Artificial Intelligence Integration on Cybersecurity: A Comprehensive Analysis. *Journal of Industrial Intelligence*, 2(2), 73-93. https://doi.org/10.56578/jii020202
12. Grant Thornton. (2025). *Does the DPDP Act lay new guardrails for India's AI ecosystem?* https://www.grantthornton.in/insights/articles/does-the-dpdp-act-lay-new-guardrails-for-indias-ai-ecosystem/
13. Group-IB. (2026). *AI Security Risks 2026 Guide*. Group-IB Blog. https://www.group-ib.com/blog/ai-security-risks/
14. Hogan Lovells. (2025). *India's Digital Personal Data Protection Act 2023 Brought into Force*. https://www.hoganlovells.com/en/publications/indias-digital-personal-data-protection-act-2023-brought-into-force-
15. IAPP. (2025). *Operational impacts of India's DPDPA*. International Association of Privacy Professionals. https://iapp.org/resources/article/operational-impacts-of-indias-dpdpa-part10
16. IBM. (2025). *Cybersecurity trends and predictions for 2026*. IBM Think. https://www.ibm.com/think/news/cybersecurity-trends-predictions-2026
17. IDC / Fortinet. (2025). *AI Adoption in Cybersecurity Surges Across India: 94% Already Using It*. SME Channels. https://www.smechannels.com/ai-adoption-in-cybersecurity-surges-across-india-94-already-using-it/
18. International Journal of Advanced Computer Science and Applications (IJACSA). (2026). *Organizational AI Readiness through the TOE Framework*. https://thesai.org/feed/oai
19. KPMG. (2026). *Cyber Security Consulting and DPDPA Compliance*. KPMG India. https://kpmg.com/in/en/services/advisory/consulting/cyber-security.html
20. Kumar, A. (2025). Machine Learning based Intrusion Detection System. *International Journal of Computer Applications*. https://www.ijcaonline.org/archives/volume187/number41/kumar-2025-ijca-925729.pdf
21. Kurup, S., & Gupta, V. (2022). Factors Influencing the AI Adoption in Organizations. *Metamorphosis: A Journal of Management Research*, 21(2), 129-139. https://doi.org/10.1177/09726225221124035
22. McKinsey & Company. (2026). *Superagency in the workplace: Empowering people to unlock AI's full potential at work*. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work

23. Mordor Intelligence. (2025). *India Cybersecurity Market Analysis 2025-2026*. https://www.mordorintelligence.com/industry-reports/india-cybersecurity-market
24. NASSCOM. (2025). *India's AI & ML Cybersecurity Capabilities*. https://www.dsci.in/files/content/knowledge-centre/2023/India%27s-AI-%26-ML-Cybersecurity-Capabilities.pdf
25. National e-Governance Division (NeGD). (2025). *AI Security Case Study*. Digital India Corporation. (https://negd-media.digitalindiacorporation.in/wp-content/uploads/2025/11/Ready-to-upload-Final_-AI-Security-Case-Study-1.pdf)
26. PwC. (2025). *AI predictions 2026: Responsible AI moves from talk to traction*. PwC Tech Effect. https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-predictions.html
27. SentinelOne. (2026). *10 Cyber Security Trends for 2026*. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/
28. TrustArc. (2025). *DPDPA's Global Reach: Cross-Border Data & AI*. https://trustarc.com/resource/dpdpas-global-reach-cross-border-data-ai/
29. World Economic Forum (WEF). (2026). *Global Cybersecurity Outlook 2026*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf)
30. World Economic Forum (WEF). (2026). *Global Cybersecurity Outlook 2026: Regional Analysis - East Asia and Pacific*. (https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026_Regional_Analysis_East_Asia_and_Pacific.pdf)