

64% of organizations plan to adopt multi-year AI/ML roadmaps, shifting from reactive spending to strategic investment: DSCI and Palo Alto Networks Report

Report Link: <https://www.dsci.in/resource/content/state-of-AI-adoption-cyber-security-india>

National, November 05, 2025: Data Security Council of India (DSCI) along with Palo Alto Networks, today released the State of AI Adoption for Cybersecurity in India report at DSCI's annual flagship summit, AISS 2025. The analysis is based on insights derived from over 160 organizations and cyber leaders across industry.

The report sets a baseline for India Inc., examining where AI adoption stands, what organizations are investing in next, and how the AI-enabled threat landscape is changing. According to the report findings, 79% of organizations plan to integrate AI/ML into existing security and operational tools, while 40% are currently in the pilot or PoC stage of AI adoption in cybersecurity.

Organizations are adopting AI to accelerate threat detection and response, and to improve predictive analytics and proactive risk scoring. Industry such as financial institutions are embedding AI into core security functions to strengthen resilience and meet regulatory requirements. At the same time, technology and IT service providers are focusing on continuous compliance monitoring and advanced anomaly detection.

The report underscores the dual reality of cybersecurity as AI-enabled attacks are amplifying adversarial offensive capabilities, while AI-based solutions are increasingly being deployed for cyber defense measures. The key report findings include:

Emerging Threat Landscape: 31% of attacks involve AI-driven supply chain compromises and coordinated multi-vector operations, while 29% stem from autonomous malware and AI-powered zero-day exploitation.

Competency Building & Capability Prioritization: 19% of organizations emphasize AI risk awareness to detect hallucinations, bias, and data leakage risks, while 16% prioritize strong data-handling judgment for secure classification, redaction, and data-sharing practices.

- AI Security Architects and Model Validators emerge as the most critical role for 18% of organizations, highlighting the need to rigorously validate models against adversarial manipulation and drift.
- Around 15% of organizations identify AI Ethics and Policy Officers as core roles, reinforcing the importance of governance, fairness, and trust in AI systems.

Speaking at the launch of the report, Vinayak Godse, CEO, DSCI, said "India is at a critical juncture where AI is reshaping both the scale of cyber threats and the sophistication of our defenses. AI enabled attacker capabilities are rapidly increasing in scale and sophistication. Simultaneously, AI adoption for cyber security can strengthen security preparedness to navigate risk, governance, and operational readiness to predict, detect, and respond to threats in real

time. This AI adoption study, supported by Palo Alto Networks, reflects DSCI's efforts to provide organizations with insights to navigate the challenges emerging out of AI enabled attacks for offense while leveraging AI for security defense.”

“AI is at the heart of most serious security conversations in India, sometimes as the accelerator, sometimes as the adversary itself. This study, developed with DSCI, makes one thing clear: appetite and intent are high, but execution and operational discipline are lagging,” said **Swapna Bapat, Vice President and Managing Director, India & SAARC at Palo Alto Networks**. “Catching up means using AI to defend against AI, but success demands robustness. Given the dynamic nature of building and deploying AI apps, continuous red teaming of AI is an absolute must to achieve that robustness. It requires coherence: a platform that unifies signals across network, operations, and identity; Zero-Trust verification designed into every step; and humans in the loop for decisions that carry real risk. That’s how AI finally moves from shaky pilots to robust protection.”

DSCI also conducted a survey with more than 100 CXOs and cyber security experts assessing the AI adoption within organizations. Around 42% of CXO leaders believe that more than 10% of the cybersecurity budget should be focused on AI-related security. Companies are expanding internal training capabilities within organization to make the workforce cyber ready for AI risks. 58% of CXOs report receiving internal training or communications on AI-related security risks.

The report underscores strategic readiness for organisations on AI security. Around 23% of organizations identify Emerging Attack Paradigms as a key catalyst for re-evaluating their AI security strategy. Whereas around 22% of organizations cite Regulatory and Compliance shifts as major catalysts influencing their AI security strategy.

About Data Security Council of India (DSCI)

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by Nasscom, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: www.dsci.in