DSCI
PROMOTING DATA PROTECTION

DSCI Digest

January 2026

DSCI Digest

The DSCI Digest is brought to you for a supporting understanding of the industry-relevant studies conducted by DSCI. It aims to help you learn and understand the subjects in discussion in a succinct composition.

Table of Contents

Indian Cybersecurity Product Landscape 3.0

"The global cyber security product market, valued at USD 239 billion in 2025, is projected to reach nearly USD 429 billion by 2030."

The global cyber security product market, valued at USD 239 billion in 2025, is projected to reach nearly USD 429 billion by 2030, pacing steadily as digital economies expand worldwide. This trajectory highlights not only the increase in security investments but also the expanding strategic importance of cyber security.

Before 2020, the cyber security product market was already on a steady growth trajectory, driven by expanding online services, accelerating digitalisation across industries, and the gradual strengthening of regulatory and compliance frameworks. Growth was steady but modest as organisations treated security as an IT cost centre rather than a board-level strategic priority. The pandemic was a turning point. Rapid, large-scale remote work, dramatic increase in cloud adoption, and stress on legacy controls exposed new attack surfaces and operational gaps. Thus, prompting acceleration in cyber security priorities and budgets. That sudden surge in demand created an unusually fertile period for cyber security product providers.

This led to the growth of the Indian cyber security product market, which can be explained through four key phases:

- Widespread digital adoption, remote work, cloud migration, and increased cyberattacks during and after the pandemic.
- Increasing trust in Indian products driven by better technical sophistication and competitive pricing.
- Expansion into higher-value product categories.
- End-user enterprises investing strategically in cyber security.

India's tryst with cyber security began quietly in the late 1970s and early 1980s, when computers first entered banks, defence research labs, and government offices. The post-

pandemic period then propelled the Indian cyber security product industry to evolve and grow further. The conversation shifted from "how to prevent breaches" to "how to build cyber resilience." India today stands as not just a consumer but also a global contributor in the cyber security product landscape.

India witnessed a rapid and sustained growth trajectory, expanding from USD 1.05 billion in 2020 to USD 4.46 billion by 2025 achieving a CAGR of 34%.

When analysing the revenue of the overall cyber security industry, the distribution of spending across industries is highly varied with BFSI and IT/ITES dominating cyber security spending, followed by Government & Public Sector, Defence & Aerospace, Retail & E-commerce, and Education & Research Institutions; Energy & Utilities, Transportation & Logistics, Real Estate & Smart Infrastructure, Media & Entertainment, and Hospitality & Travel; and lastly Manufacturing & Industrial/OT Security, Telecommunications, Healthcare & Life Sciences.

This reflects a complex interplay of regulatory mandates, digital transformation maturity, threat exposure, and the criticality of data protection to business operations leading to the varied distribution.

To meet evolving enterprise requirements, significant portion of Indian cyber security providers have shifted towards offering multiple delivery alternatives because enterprises now demand flexible, cloud-ready, hybrid, and on-premise options to align with diverse infrastructure needs, regulatory obligations, and risk postures, making multi-delivery support essential for scalability, global competitiveness, and customer adoption.

Deployment and delivery represent the critical final mile in bringing cyber security products to end users, determining not just how protection is installed, but how effectively it can be managed, scaled, and maintained over time. The chosen delivery method directly impacts implementation speed, operational overhead, total

cost of ownership, and the organisation's ability to respond to emerging threats.

The Go-to-Market (GTM) strategy of Indian cyber security product companies is therefore heavily partner-centric, where 55% of Indian cyber security product companies have established a global footprint. This scenario looms large as the strategy in place works towards enabling scalability, especially for smaller or mid-sized cyber security firms looking to grow internationally without overextending resources. India's licensing model for cyber security products currently includes:

- Subscription license
- Perpetual license
- Usage-based license
- Freemium
- Pay-per-use license

Furthermore, the support ecosystem entails initiatives from both the central and state governments along with policy support. The industry is also well supported by industry bodies and multiple centres of excellence. Considerations are also in line for investing in dedicated R&D teams and setting aside specific budgets for intellectual property development. Interestingly, 115 patents were filed by Indian cyber security product companies in year 2024-25. Collaborating with academic institutions, participating in co-innovation programs, and engaging with government-backed incubators can provide valuable access to research talent and innovation ecosystems.

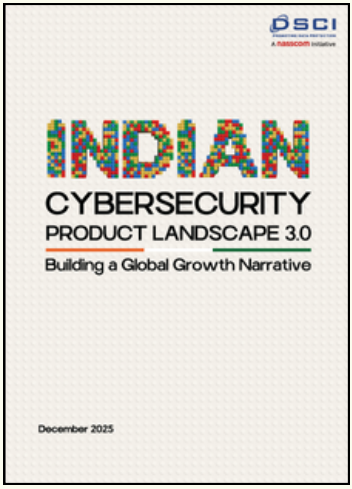
Additionally, fostering an internal culture that rewards patentable innovations, aligning IP planning with product development strategies, and seeking guidance from IP experts early in the process can help enhance the quality and frequency of filings.

For continued growth in the ecosystem, the Indian cyber security product companies currently employ approximately 60,000 professionals. With plans to expand the talent pool by close to 25% annually. Yet finding and placing the right talent remains a challenge. The cyber security market is undergoing rapid platform convergence, driven by the need for integrated security,

operational efficiency, and reduced vendor complexity. While analysing the future priorities, Indian cyber security product companies reveal an inflection point: oscillating between ambitious global aspirations and pragmatic domestic consolidation. The sentiment is optimistic yet operationally grounded, with companies recognizing that customer acquisition, product innovation, and brand building must precede international expansion.
Therefore, the three dominant themes that emerge are:

- Domestic customer acquisition as the immediate growth engine.
- Global business expansion as the strategic ambition.
- R&D innovation and new product development as the differentiator.

Indian cyber security product companies reflect a growing level of maturity, establishing India as a reliable and competitive player in emerging, high-value cyber security domains with accelerating global demand. The discussed facets are detailed in the report on 'Indian Cybersecurity Product Landscape 3.0'.



Read the entire report

State of AI Adoption for Cyber Security in India

"Around 79% of organisations are accelerating the adoption of AI-driven capabilities within their existing security infrastructure."

AI has emerged as the cornerstone of next-generation cyber security. Today, organisations seek measurable impact against experimentations in areas such as faster threat detection, lower false positives, and stronger operational resilience.

Investment intent is also rising sharply, reflecting recognition of the fact that human-centric defence models alone cannot match modern attack velocity. The motivation driving this is both defensive and strategic.

AI/ML deployment for cyber security is attaining significant pace across technology/IT, BFSI, and government sectors. But the foremost AI deployment target transforming cyber security operations that are overwhelmed by escalating alert volumes and adversaries leveraging offensive AI.
Key objectives to deploy AI/ML within the cyber security function include:

- Accelerating threat detection and response through real-time AI-driven automation.
- Usage of predictive AI for proactive risk identification, transforming cyber security from reactive defence to anticipatory defence.
- Constant real-time monitoring of an organisation's adherence to regulations, standards and policies beyond periodic audits.

However, AI adoption for cyber security is not uniform, it is largely tailored to sectoral risks, regulatory pressures, and organisational maturity. From a strategic leadership standpoint, cyber security is now being redefined through the lens of AI, not just as a tool, but as a force multiplier that enhances operational efficiency, improves risk governance, and builds long-term enterprise resilience. AI is playing a pivotal role in making cyber security more transparent, explainable, and boardroom-ready.

It is enabling better visibility across complex environments while simultaneously driving the evolution of traditional SOC into autonomous, self-learning defence platforms.

Together, these strategic shifts signal a decisive move from tactical adoption to organisation-wide AI integration. In response to increasing threat complexity and regulatory demands, organisations are accelerating the adoption of AI-driven capabilities (~79%) within their existing security infrastructure. Moreover, majority of organisations (~64%) are now investing proactively, aligning their AI initiatives with multi-year risk management roadmaps.

But AI's transformative power cuts both ways. The same intelligence used to defend is now weaponised to breach them. Attackers are leveraging generative models, automated reconnaissance, and adaptive malware to dismantle traditional controls at machine speed.

Some of the identified AI-enabled attacker capabilities with greatest strategic and operational risks to organisations are:

- AI-poisoned supply chains/backdoor models (manipulated training data or third-party model backdoors).
- Autonomous/polymorphic malware (self-adapting malware that evolves using ML/ Reinforcement Learning).
- Deepfake social engineering at scale (AI voice/video/text impersonation of executives for fraud).
- Coordinated multi-vector AI attacks (orchestrated simultaneous attacks across network, data, identity & physical domains).
- AI-driven zero-day discovery and weaponisation (finding/exploiting vulnerabilities faster than patching).
- Synthetic identity fraud (AI-generated identities that pass verification/KYC).
- Prompt injection & LLM/ GenAI abuse (manipulating LLMs to bypass controls or exfiltrate data).

Traditional security models are proving insufficient against these threat vectors. Business verticals like Finance and Human Resources teams face the highest AI-enabled attacks (based on success rate)

due to their natural exposure to social-engineering interactions, limited training on advanced AI-driven threats, and focus on business operations over cyber security. Followed by them are the Sales/Customer Relations, Marketing, and Partner-Ecosystem teams due to their high exposure to external interaction, multi-device work patterns, and heavy dependence on third-party SaaS tools and APIs.

The path to AI-enabled security maturity remains constrained by structural and operational gaps. Skilled AI-security talent is scarce, data pipelines are fragmented, and infrastructure scalability often lags in ambition.

Moreover, organisations aiming to operationalise AI for cyber security often face stalled progress due to persistent barriers, including high financial commitments, talent gaps and architectural constraints.

The increasing use of AI in cyber security is compelling organisations to re-assess their risk appetite and balance innovation. In addition, CXOs view AI adoption in cyber security through a dual lens, where on one end it is unlocking opportunities in speed, scale, and automation, and on the other end it is enabling confronting exposures related to governance, data breaches, and reliability without compromising security. The focus has shifted towards developing specialised talent that blends security acumen with AI fluency, while investing in architectures capable of real-time learning and adaptation.

Building resilient AI security now hinges on how effectively organisations unify skills, systems, and culture to scale trusted, intelligent defence. Emerging priorities today include AI risk awareness, data handling judgment and human-in-the-loop governance, prompt discipline, and vendor and tool evaluations.

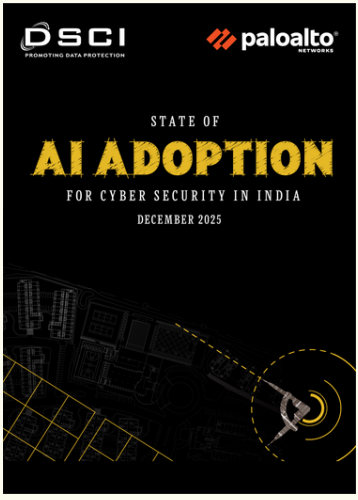
Organisations are re-architecting their cyber security environments by embedding AI-driven intelligence, adaptability, and resilience into the core design of their defence stacks.

Forward-looking CISOs are architecting hybrid models that merge local data control with cloud scale intelligence, ensuring both speed and sovereignty. Investments are directed towards adaptive platforms that learn continuously while maintaining resilience and compliance.

It is also important to note that as organisations embed AI into cyber security operations, the focus is shifting from using AI for security to securing AI itself. Achieving resilient, AI-enabled cyber security requires implementing strong technical controls, through model integrity validation, access governance, adversarial defence mechanisms, and more.

Similarly, transnational AI advancements reflect a growing recognition among governments to establish robust regulatory and operational frameworks that ensure responsible and secure deployment of artificial intelligence in cyber security.

More details on the subject can be found in the report on 'State of AI Adoption for Cyber Security in India.'



Read the entire report

Safeguarding India's Digital Health

A Framework for Cybersecure Healthcare Infrastructure

"The healthcare industry has become one of the most targeted sectors where it recorded the highest average cost of a breach at over USD 7.42 million per incident."

India's healthcare ecosystem is undergoing rapid digital transformation. Driven by initiatives such as the Ayushman Bharat Digital Mission (ABDM) and the increasing integration of Electronic Health Records (EHRs), telemedicine, and Internet of Medical Things (IoMT), healthcare providers are leveraging technology to improve accessibility, quality, and efficiency. However, this digital progress has also expanded the cyberattack surface, making cyber security and data privacy essential components of a trusted healthcare system.

The healthcare industry has become one of the most targeted sectors where it recorded the highest average cost of a breach at over USD 7.42 million per incident. The dramatic rise in cyberattacks in the country, driven by rapid digital transformation, has outpaced the security readiness. The healthcare sector accounted for nearly 21.82% of all malware attacks, a stark increase from previous years (8% in 2023).

Therefore, securing healthcare infrastructure demands a comprehensive cyber security framework that integrates technology upgrades with governance, accountability, and capacity building.

The attack vectors that target today range from primary threats like phishing and social engineering, to complex threats like API exploits & interface abuse to emerging threats like AI-assisted attacks. Stakeholders can benefit from this bifurcation of threats and build a security posture that not only prevents financial and reputational damage but also safeguards patient safety and trust in the digital health ecosystem.

The healthcare landscape can be broken down into three lenses for better framing of the required cyber security framework. This includes:

• People – They represent healthcare professionals, administrators, and patients who interact with digital systems daily. Their awareness and digital hygiene form the first line of defence.

• Providers - They encompass hospitals, laboratories, clinics, and healthtech startups responsible for securing IT infrastructure, connected devices, and patient data.

• Health Systems- These include regulators, policymakers, and public health institutions that shape the governance and standards of digital security.

Evaluation of varying levels of preparedness through these three lenses can help formulate an understanding of the digital maturity of the current ecosystem.

Assessing IT infrastructure & data value chain risks also becomes crucial as it forms the backbone of the modern care delivery. Any single point of failure in the interconnected ecosystem can have cascading impacts on service continuity, patient safety and create new vulnerabilities.

Misconfigured networks, outdated servers, poorly secured endpoints, and weak cloud governance can provide attackers with multiple entry points. Understanding and mapping these risks across the healthcare data value chain and overall IT infrastructure is essential to designing a resilient cyber security strategy.

However, securing healthcare IT infrastructure is challenging due to its complex mix of legacy systems, cloud platforms, and connected medical devices. Limited resources, skill shortages, and reliance on third-party vendors add to the difficulty.

It is important to consider that digital health risks and responsibilities are distributed among people, providers and healthcare systems across the data value chains of data generation, data transmission, data storage, data usage and processing, data sharing and exchange, and data archival and disposal. A robust, integrated approach to data security across IT, OT, and connected medical and biomedical devices will further strengthen cyber resilience.

Today for healthcare sector, cyber security, data security and privacy have become inseparable and interdependent pillars of digital trust. Addressing them in silos will lead to incomplete protection. A unified approach to securing healthcare IT infrastructure should treat privacy as a strategic design element within the cyber security architecture. This means adopting privacy-by-design and security-by-design principles together, where technical safeguards (such as encryption, access controls, and audit trails) are complemented by robust privacy practices (such as consent logs, data minimisation, and breach notification mechanisms).

Similarly, aligning with global standards can help Indian healthcare providers benchmark their privacy posture against global peers, prepare for cross-border collaborations, and move towards adopting a 'privacy-by-design' approach. Some of the notable global standards to be considered include:

• ISO/IEC 27701 (Privacy Information Management System – PIMS)
• NIST Cybersecurity Framework (CSF) 2.0 and NIST Privacy Framework
• HIPAA Privacy and Security Rules and HIPAA Breach Notification Rule
• IEC 80001-1 (Risk Management for Medical IT Networks)
• General Data Protection Regulation (GDPR)
• Payment Card Industry Data Security Standards (PCI DSS)

Together, these international frameworks and standards provide a foundation to future-ready privacy posture for Indian healthcare organiations. They act as a bridge between India's domestic frameworks (DPDPA, 2023, ABDM) and global expectations.

Moreover, cyber security, privacy and data protection must be viewed through a single, unified lens rather than as independent compliance or technical functions. These three domains are deeply interdependent and collectively form the foundation of patient trust and systemic resilience.
Threat landscapes evolve rapidly, with adversaries constantly developing new tools and exploiting emerging

vulnerabilities. A security program that remains static quickly becomes obsolete, leaving organisations exposed despite past investments. Regular reassessment of policies, controls, and incident response mechanisms ensures alignment with current risks, technological advancements, and compliance mandates.

Therefore, a Healthcare Cybersecurity Readiness Framework tailored to India's healthcare cyber security context has been designed in the latest report on 'Safeguarding India's Digital Health: A Framework for Cyber Secure Healthcare Infrastructure' that assesses readiness across access, capability, and trust. It also allows providers to benchmark their cyber security maturity and chart pathways for improvement.

Read the entire report

What to Expect in the Next Edition

The DSCI Digest offers a condensed version of all our publications, giving you a quick overview to help you decide on your next read.

The subjects catered here enable you to gain first-hand information on the volumes we bring out for the industry. The information shared is a brief account of the conducted studies. You are requested to visit the reports on our website for better understanding.

https://www.dsci.in/knowledge-center/study-and-reports

Authors

- "Indian Cybersecurity Product Landscape 3.0" by Anuprita Singh and Neha Mishra
- "State of AI Adoption for Cyber Security in India" by Priya Sharma and Neha Mishra
- "Safeguarding India's Digital Health: A Framework for Cybersecure Healthcare Infrastructure" by Anuprita Singh and Neha Mishra

Compiler and Editor

Mridushi Bose, Senior Associate

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by Nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit https://www.dsci.in/

DATA SECURITY COUNCIL OF INDIA
NASSCOM CAMPUS, FOURTH FLOOR, PLOT. NO.
7-10, SECTOR 126, NOIDA, UP - 201303
+91-120-4990253 | INFO@DSCI.IN | WWW.DSCI.IN

dsci.connect dsci.connect dscivideo data-security-council-of-india DSCI_Connect