

Cyber Threats Escalate Across Indian Financial Institutions as AI Reshapes the Cybersecurity Landscape

- 1) AI has rewritten attacker economics globally, with exploit windows collapsing from 745 to 44 days and attack costs falling over 70 percent; a survey of Indian BFSI CISOs revealed a strong intent to action for mitigating the AI enabled cyber threats.
- 2) Nearly 70% CISOs expect significant impact of AI within 12 months. However, confidence in organisational readiness to withstand an AI-enabled breach remains limited.
- 3) Over 70% of Indian BFSI organisations surveyed have deployed AI-assisted SOC capabilities or are operating at higher maturity levels
- 4) Over 40% of Indian CISOs recognize that attackers are already moving faster than their defenses
- 5) Report calls for Indian BFSI to shift from compliance-led cybersecurity strategy to synchronized resilience, aligning defense across business risk, cross-functional teams, solution providers, people, and the wider ecosystem

NATIONAL, 28 MAY 2026: Data Security Council of India (DSCI) and Boston Consulting Group (BCG) today released "Cybersecurity in the Age of AI: Building a Synchronous BFSI Enterprise," a comprehensive report on how AI is reshaping cybersecurity risk across India's banking, financial services, and insurance sector. Drawing on a DSCI-BCG Indian CISO Survey of 42 senior security leaders and direct face-to-face interviews, the report finds India's BFSI organisations experience cyber-attacks at 1.6 times the global average, with reported incidents more than doubling in four years — from 1.4 million in 2021 to 2.9 million in 2025. Mean time to contain a breach in India stands at 263 days and is still climbing. Mid-size organisations face the sharpest exposure: having digitized aggressively and built deep interconnections across the financial system, they carry the risk profile of large players with a fraction of the cyber investment to match it.

The report further notes, every BFSI institution must now simultaneously curb AI-powered attacks, deploy AI for defense, and secure its own AI systems — as a synchronous effort. Indian BFSI sector is undergoing a transformation. The sector has been operating on traditional cyber models - where threats evolved over months, and were easier to track, digital journeys were simpler, and the CISO could largely coordinate the response from within the security function. But this needs to change, and quickly. Cyber resilience can no longer be managed as a security-function agenda.

The attack surface has become too distributed for any single function to defend. When business, IT, risk, compliance, and security move at different speeds, digital and AI-led innovation can outpace the safeguards designed to protect it. The next cyber operating model for Indian BFSI must therefore shift from a control-led function to a synchronized resilience system.

Vinayak Godse, CEO, Data Security Council of India (DSCI), at the launch said, *“Frontier AI is accelerating the convergence of cyber risk, digital scale and business resilience in BFSI —the ability to secure AI-driven operations will define the sector's future trust and competitiveness.*

The next frontier is autonomous defence: AI-driven detection and response operating at the same machine speed as the attacks we now face, with agentic security architectures redefining how institutions manage risk at scale, shifting analysts from triage to strategic oversight.”

Nisha Bachani, Managing Director and Partner, Boston Consulting Group, said, *“AI has rewritten the economics and compressed the window of cyber-attacks. Time to exploit has collapsed by more than 90%, and the cost of mounting a sophisticated attack has fallen by over 70%. However, defender cycles are still catching up, and patching to change management takes from weeks to months. This asymmetry between speed of attack and remediation is the real challenge, and it falls hardest on ‘Mid-tier organisations’ - where risk is material, but investments might not be proportionate yet.*

The institutions that move decisively over the next twelve to eighteen months will define the real industry moat. The answer is not just controls but a synchronous defense posture: where Cyber is aligned with business risk, tech, legal, third party and the wider ecosystem”

Report brief:

1. AI driven cyber risk has become a defining strategic concern for Indian BFSI, and the sector is responding at pace: 76 percent of CISOs rank AI enabled attacks among their top four priorities for 2026. 90 percent have already reshaped cyber spending to address AI, against 74 percent globally. 83 percent are embedding AI into cyber operations, and 71 percent have reached AI assisted maturity in their security operations centre, with 38 percent operating with trust in autonomous decisions or fully agentic levels The momentum is evident, but significant work remains. AI specific controls such as formal AI governance, agent monitoring and runtime guardrails are still being built across the sector, and operational confidence in AI breach readiness continues to mature. Leading Indian institutions are moving in step with the global frontier, and the next 12 to 18 months will determine how widely that leadership extends.
2. Years of sustained regulatory engagement have built one of the strongest cyber baselines in global financial services: The regulatory load is significant, with more than 60 percent of leaders citing overlapping mandates as a meaningful demand on cyber resources. That engagement has, however, produced a structural payoff. 79 percent of Indian BFSI institutions operate data protection at active or continuous maturity, the highest of any cyber discipline measured, and 75 percent have reached the same level on monitoring and detection. The average cost of a data breach in Indian BFSI is materially lower than the

global benchmark. The next chapter is to extend the same discipline to areas where maturity is still developing, including third party risk, governance and AI specific controls, turning compliance into a durable security advantage.

3. The path forward is not more controls. It is synchronicity: Indian BFSI's next cyber operating model must shift from a security function agenda to a synchronized resilience system across five fronts. Cyber priorities must follow business risk. Business, risk, legal, technology and security teams must operate with shared accountability. Third parties must be governed as extensions of the enterprise. Insider risk and customer fraud must be addressed as one program. Threat intelligence must be shared across peers and regulators as a collective asset rather than an institutional one.

The full report, **Cybersecurity in the Age of AI: Building a Synchronous BFSI Enterprise**, is available here: <https://www.dsci.in/resource/content/cybersecurity-in-the-age-of-AI-for-BFSI>





About Boston Consulting Group (BCG)

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders, empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact. Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

About DSCI

Data Security Council of India (DSCI) is a not-for-profit, think tank on data protection, cyber security and critical technologies 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, law enforcement agencies, defence, industry sectors including IT-BPM, BFSI, CII, Telecom, and other think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: www.dsci.in



Media Contacts

BCG India: Bhumika Gupta | gupta.bhumika@bcg.com | 9818096329

DSCI: Amit K Ghosh | amit.ghosh@dsci.in | 9899113136