Ministry of Electronics & IT

MeitY releases 2nd edition of the Digital Threat Report 2025-26 for India's BFSI Sector in Collaboration with SISA

Report Highlights AI Asymmetry and Emerging Cyber Trends to Strengthen Security and Resilience in India's BFSI and Payments Ecosystem

Posted On: 13 JUL 2026 1:59PM by PIB Delhi

The Ministry of Electronics and Information Technology (MeitY), along with the Indian Computer Emergency Response Team (CERT-In), the Computer Security Incident Response Team in Finance (CSIRT-Fin) and SISA, today released the second edition of the **Digital Threat Report 2025–26** for the Banking, Financial Services and Insurance (BFSI) and payments ecosystem. The report provides financial institutions, regulators and cybersecurity leaders with an executive assessment of the threats reshaping banking, financial services, insurance and digital payments.

Addressing the gathering at the launch of the report, Shri. S. Krishnan, Secretary MeitY said, “As cyber threats become increasingly sophisticated, trusted partnerships between public institutions and industry are essential to strengthening digital trust. The Digital Threat Report represents a meaningful collaboration among CERT-In, CSIRT-Fin and SISA. This partnership demonstrates how expertise developed in India can contribute both to our national cyber resilience and to advancing cybersecurity knowledge globally."

The report draws on extensive digital forensics and incident response (DFIR) research, analysis aligned with CERT-In and CSIRT-Fin observations, and research into adversarial AI. Its central finding is that six of the seven forward-looking predictions made in last year's edition have already reached full-scale realization. This rapid progression demonstrates how the time between the emergence of a threat and its operational exploitation is shrinking, often from years to months or even weeks.

Threats previously considered emerging or episodic - including social engineering, credential theft, supply-chain compromise and cloud exploitation - are now established attack methods. The consequence is a threat environment where the most damaging attacks no longer resemble traditional intrusions at all. They surface as legitimate sessions, approved payments, manipulated workflows, or ordinary user behaviour that are indistinguishable from genuine activity until the damage is already done.

"The distance between innovation and exploitation has narrowed dramatically, and that single shift changes everything about how our industry must defend itself," said *Dharshan Shanthamurthy, Founder & CEO of SISA*. "The BFSI industry is built on trust - trust that a transaction is genuine, that the systems processing it are acting as intended, that money will move securely and irreversibly through a network of institutions that depend on one another. When that trust is weakened, the impact is never contained to a single breach or a single firm; it ripples across customers, partners, markets, and entire economies. This is why cybersecurity can no longer sit at the edge of the business as a technical control function. It has to become central to how institutions grow, innovate, and lead. Our work in forensics has taught us a simple truth: every breach leaves behind a lesson, and if we are willing to learn fast enough, those lessons can turn disruption into foresight."

The report identifies **AI asymmetry** as one of the defining risks facing financial institutions. Activities that once required specialist teams, significant resources and weeks of effort can increasingly be performed at machine speed by comparatively low-resource threat actors. This is placing offensive capabilities on a faster development curve than many of the defensive and regulatory mechanisms designed to contain them.

“We are pleased to collaborate with SISA for the second consecutive year on the Digital Threat Report for the BFSI Industry,” said Dr. Sanjay Bahl, Director General, CERT-In. “As India’s financial ecosystem becomes more interconnected, real-time and technology-driven, cyber resilience must be treated as a shared responsibility across institutions, regulators and the wider digital supply chain. The report highlights the need to move beyond periodic security interventions towards continuous risk assessment, coordinated response and stronger information sharing. By translating emerging threat patterns into actionable guidance, it aims to help financial institutions anticipate systemic risks, strengthen operational resilience and protect trust in the country’s digital financial infrastructure.”

To help leaders steering enterprise security understand why well-established controls still fail under real-world pressure, the report looks beyond individual incidents to examine the conditions that allow breaches to escalate. A standout of this edition is the Anatomy of Cyber Failure - a 4-Layer Gap Archetype Framework that reconstructs, end to end, how a modern breach actually happens. Seen through this lens, a breach is rarely a single lapse but a chain of compounding weaknesses, helping organizations identify recurring patterns, prioritize systemic risks and direct investments toward the gaps with the greatest potential impact.

Envisioned to move from findings to foresight, the report converts this diagnosis into direction. For the industry and institutions, it identifies the shifts likely to reshape the sector and sets out an 18-month roadmap - moving from strengthening foundational controls to building continuous capabilities and, ultimately, more resilient security architectures.

The 2025-26 Digital Threat Report is available at [link].

About CERT-In

CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. In the Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed

For more details: www.cert-in.org.in.

About CSIRT-Fin

Computer Security Incident Response Team in Finance sector (CSIRT-Fin), is a nodal sectoral CSIRT which provides Incident Prevention and Response services as well as Security Quality Management Services to the entities of the Indian financial sector. It manages cyber incidents and coordinate responses across banking, securities market infrastructure, insurance, and pension funds entities. It carries out the following roles related to the cyber security in financial sector:

- Collection, analysis & dissemination of information on cyber incidents.
- Forecast and alerts on cyber security incidents.
- Emergency measures on cyber security incidents.
- Coordination for cyber incident response activities.
- Issue guidelines, advisories, vulnerability, and white papers relating to information security.
- Monitor sectoral efforts in the financial sector towards maintaining dynamic and modern cyber security architecture, developing awareness amongst regulated entities and public in general.
- Such other functions relating to cyber security in the financial sector, as may be prescribed.

About SISA

SISA is a global leader in cybersecurity for the payment ecosystem, operating at the intersection of **AI, cybersecurity, and payments**. Trusted by leading brands and financial institutions across **40+ countries**, SISA secures over **1,000 organizations** by helping them anticipate threats, strengthen resilience, and protect critical payment infrastructure. Powered by **real-world breach intelligence,** SISA enables organizations to stay ahead of evolving cyber risks. Follow SISA on LinkedIn for the latest insights on cybersecurity, payment security innovation, and emerging technologies.

For more details: www.sisa.ai.

****

Dharmendra Tewari / Kanishk Sharma / Vanshita Jaiswal