Digital Threat Report 2025-26

Prelims: *Current events of national and international importance | Science & Technology | Cybersecurity*

Why in News?

Recently, the Ministry of Electronics and Information Technology (MeitY), along with CERT-In, CSIRT-Fin, and SISA, released the 2nd edition of the Digital Threat Report 2025-26.

- **Digital Threat Report –** The report gives financial institutions, regulators, and cybersecurity leaders a clear overview of threats affecting banking, insurance, and digital payments.

Key Highlights

- The report highlights AI asymmetry and emerging cyber trends reshaping financial security for India's Banking, Financial Services and Insurance (BFSI) and payments ecosystems.
- **Rapid Threat Evolution –** Six of seven predictions from last year's report have already materialised.
- Shrinking gap between threat emergence and exploitation (from years to months/weeks).
- **Established Attack Methods –** Social engineering, credential theft, supply-chain compromise, and cloud exploitation are now mainstream.
- Modern attacks blend into normal activities (like logins or payments), making them look legitimate and very difficult to spot before damage happens.
- **Cyber Resilience –** India's financial system is highly connected, so one breach can spread across markets and economies.
- The report calls for ongoing risk checks, real-time responses, and information sharing instead of occasional audits.
- **Nature of Attacks –** Breaches often appear as legitimate sessions, approved payments, manipulated workflows, or ordinary user behaviour, making detection harder.

- **AI Asymmetry –** Low-resource attackers can now use AI to perform activities at machine speed, outpacing defensive and regulatory mechanisms.
- **Anatomy of Cyber Failure –** Introduces a ***4-Layer Gap Archetype Framework,*** to analyse how modern breaches escalate.
- A major cyber failure is not caused by one weakness but by a chain of small gaps.
- **Roadmap –** Sets an 18-month plan to guide financial institutions from basic security controls to building continuous, resilient security systems

Institutional Roles

- **Indian Computer Emergency Response Team (CERT-In) –** National nodal agency under IT Amendment Act 2008 for responding to computer security incidents.
- **Computer Security Incident Response Team in Finance (CSIRT-Fin) –** A nodal sectoral CSIRT for India's financial sector that provides incident prevention, response, and security quality management services.
- **SISA –** Global cybersecurity leader for the payments ecosystem; secures 1,000+ organisations across 40+ countries using breach intelligence and AI-driven solutions.

Reference

PIB | Digital Threat Report 2025-26