GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 722
TO BE ANSWERED ON: 05.12.2025

RISING COSTS OF DATA BREACH

722. SMT. PRIYANKA CHATURVEDI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether Ministry is aware of recent report indicating that average cost of a data breach in India surged to ₹22 crore in 2025;
(b) if so, whether Ministry has analysed key drivers of this increase and findings thereon;
(c) whether Ministry plans to issue or strengthen regulations requiring stronger AI access controls, mandatory AI-governance frameworks, and security audits, particularly for organisations deploying generative AI or other advanced AI systems; and
(d) whether Ministry will propose or support financial incentives for Indian companies to invest in security AI, automation, and responsible governance practices to mitigate risk of data breaches in the era of rapid AI adoption?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): The Government is cognizant of the cyber threats to India's digital infrastructure. Agencies involved in cybersecurity regularly study the reports published by cybersecurity experts, companies and academic institutions.

The government has released the India AI Governance Guidelines, a comprehensive roadmap for safe, inclusive, and responsible AI use. The Guidelines rest on seven guiding principles (sutras): Trust, People First, Innovation over Restraint, Fairness and Equity, Accountability, Understandable-by-Design, and Safety, Resilience and Sustainability. They adopt a risk-based, sector-aware governance model, relying on existing legislation along with targeted amendments instead of creating a single umbrella AI law.

In addition, Digital Personal Data Protection Act, 2023 ('the Act') establishes the legal framework governing the processing of digital personal data in India. The Act and Digital Personal Data Protection Rules, 2025 have been notified on 14 November 2025.

The Act requires all Data Fiduciaries to ensure responsible processing of personal data, with clear obligations relating to transparency, purpose limitation, data minimisation, accuracy, security safeguards, timely erasure, and respect for the rights of Data Principals. It mandates prompt notification of personal data breaches to both affected individuals and the Data Protection Board of India.

Further, the Government has undertaken following initiatives to prevent cyber threats including risk of data breaches in the era of rapid AI adoption, which inter alia includes:

i. CERT-In has issued a cyber security baseline document, in September 2025, which provides a minimum set of security controls recommended for Micro, Small and Medium Enterprises

(MSMEs). This helps MSMEs to implement essential measures for strengthening their cyber security posture.

ii. National Cyber Coordination Centre (NCCC), implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.

iii. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same. It also provides cyber security tips and best practices for citizens and organisations.

iv. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of various organisations.

v. CERT-In has empanelled 231 security auditing organizations to support and audit implementation of Information Security Best Practices.

vi. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis.

vii. CERT-In has issued updated technical guidelines in July 2025 for Bill of Materials (BOM) for software, hardware, Artificial Intelligence, Quantum Computing & Cryptography requirements. These guidelines are aimed to enhance the security and transparency of supply chains for software, hardware & emerging technologies.

viii. The Certified Security Professional in Artificial Intelligence (CSPAI) program was launched by CERT-In in September 2024. The program aims to address the growing need for Secure and Responsible AI integration into business applications and processes. The CSPAI program equips cybersecurity professionals with the skills to secure AI systems, proactively address AI-related threats, and ensure trustworthy AI deployment in business environments.

ix. CERT-In has published “Cyber Security Guidelines for Smart City Infrastructure” in February 2025 including measures for secure usage of Artificial Intelligence (AI) and Machine Learning (ML) for smart city infrastructure and applications.

******