GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 707
TO BE ANSWERED ON: 05.12.2025

CYBER SECURITY AND DATA BREACHES TARGETING
PRIVATE COMPANIES

707.   SHRI S NIRANJAN REDDY:

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

(a) whether Government is aware of increasing number of cyber attacks and data breaches targeting private companies in India;
(b) if so, the number of such incidents reported annually to the Indian Computer Emergency Response Team (CERT-In) over the last 5 years;
(c) whether any assessment has been made regarding the nature of data compromised, including personal, financial, or business-sensitive information in these cyber incidents;
(d) whether there exist mandatory minimum standards or guidelines for private companies to ensure data privacy and protection against cyber threats; and
(e) if so, the details thereof, and if not, the reasons therefor?

ANSWER

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

(a) to (e): The Government is cognizant of cyber threats, challenges faced by Indian government and private sector entities. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology (IT) Act, 2000.

Cyber security incidents related to private sector organisations observed by CERT-In during the last five years are given below:

Year	Incidents
2020	11,03,894
2021	13,54,524
2022	11,99,018
2023	13,88,073
2024	7,31,988

The Government has undertaken various initiatives for organisations including private companies to ensure data privacy and protection against cyber threats, which inter alia, include:

i. The Digital Personal Data Protection Act, 2023 and Rules made thereunder establish the legal framework governing the processing of digital personal data. It casts an obligation relating on 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

ii. 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.

iii. 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.

iv. 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.

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

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

vii. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.

viii. CERT-In conducts regular cyber security trainings for IT/ cyber security professionals of Government, public and private sector organizations.

ix. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

******