GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 703
TO BE ANSWERED ON: 24.07.2026

CYBER SECURITY INCIDENTS AND STRENGTHENING OF CYBERSECURITY INFRASTRUCTURE

703. SHRI JOSE K. MANI:

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

(a) whether Government has maintained data on cyber security incidents reported during the last three years;
(b) if so, the year-wise and sector-wise details thereof, including attacks on Government institutions, financial institutions and critical infrastructure;
(c) the number of incidents successfully mitigated and cases investigated; and
(d) the measures taken to strengthen the country's cyber security infrastructure and incident response mechanisms?

ANSWER

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

(a) to (d): Government is committed to ensuring an open, safe, trusted and accountable cyberspace. Several legal, technical, and administrative policy measures have been implemented to address cyber security challenges in the country.

The Government has institutionalised a nationwide integrated and coordinated system to deal with cyber-attacks in the country which, inter alia, includes:

1. 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 Act, 2000.
2. National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines the cyberspace to detect cyber security threats.
   It shares the information with concerned organisations, state governments and stakeholder agencies for taking action.
3. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
4. Cyber Swachhta Kendra (CSK): A citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space.
   It 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.

5. Sectoral Computer Security Incident Response Team (CSIRT): CSIRT in Finance sector (CSIRT-Fin) under CERT-In is operational since May 2020 to coordinate cyber incident response in the banking and financial sector
   CSIRT-Power is operational since September 2024 as an extended arm of CERT-In to coordinate cyber security issues within the power sector entities.
6. CERT-In coordinates incident response measures with affected organisations, service providers, regulators and law enforcement agencies.
7. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.
8. CERT-In has formulated Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Central Government Departments, State Governments and their organizations.
9. CERT-In has empanelled 237 security auditing organisations to support and audit implementation of Information Security Best Practices.
10. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. Workshops along with these drills are conducted in States for facilitating coordination and information sharing in the area of cyber security.
11. CERT-In has operationalised a Responsible Vulnerability Disclosure and Coordination Program for collection, analysis, mitigation and coordination with researchers/finders/vendors for fixing vulnerabilities in software/ devices.

As per the information reported to and tracked by CERT-In, the total number of cyber security incidents belonging to Government and financial institutions observed during last three years are given below:

Year	Number of cyber security incidents
2023	11,46,491
2024	18,73,270
2025	24,38,967

CERT-In also issues Advisories, Guidelines and Directions:

1. CERT-In has issued a “Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure” in May 2026, aimed at protecting digital infrastructure against rapidly evolving AI-driven cyber threats.
2. CERT-In has issued an advisory titled “Defending Against Frontier AI Driven Cyber Risks” in April 2026, outlined comprehensive measures for organizations, and individuals to strengthen protection against advanced AI-enabled threats.
3. CERT-In has issued updated technical guidelines in July 2025 for Bill of Materials (BOM) for software, hardware, Artificial Intelligence, Quantum Computing & Cryptography requirements.
4. CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.
5. CERT-In has issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

*****