GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2308
TO BE ANSWERED ON: 07.08.2026

CYBER ATTACK PREPAREDNESS

2308. DR. ASHOK KUMAR MITTAL:

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

(a) the initiatives undertaken by the Indian Computer Emergency Response Team (CERT-In) to counter rising sophisticated ransomware attacks;
(b) the total number of critical information infrastructure breaches successfully mitigated across the banking and healthcare sectors recently;
(c) whether Government has strictly enforced the mandatory six-hour cyber incident reporting guidelines for all corporate entities;
(d) the details of the nationwide simulated cyber-drill exercises conducted to evaluate the digital readiness of State power grids; and
(e) the measures implemented to deploy indigenous firewall technologies?

ANSWER

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

(a) to (e): 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 Act, 2000. The measures taken by CERT-In to strengthen cyber security and prevent cyber attacks, inter-alia, includes:

i. National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines cyberspace to detect cyber security threats. It shares the information with concerned organisations, state governments, and stakeholder agencies for taking action.
ii. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across States and sectors for proactive threat mitigation.
iii. **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.

iv. CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Central Government Departments, State Governments and their organizations.
v. CERT-In coordinates incident response measures, including for ransomware attacks, with affected organisations, service providers, regulators and law enforcement agencies.
vi. CERT-In issues alerts and advisories regarding the latest cyber threats, vulnerabilities, and ransomware attacks along with countermeasures to protect computers, networks, and data on an ongoing basis.

vii. CERT-In has detected and mitigated malicious scanning/probing incidents and vulnerable services successfully in coordination with targeted entities in the finance and healthcare sectors as given below:

Finance sector	**2025**	**2026 (upto June)**
Malicious scanning and probing	470445	309288
Vulnerable Services	99663	39319
Total	570108	348607

Healthcare sector	**2025**	**2026 (upto June)**
Malicious scanning and probing	32297	18259
Vulnerable Services	2183	596
Total	34480	18855

In addition, a total number of 39 and 17 targeted intrusion campaigns were successfully detected and mitigated across the banking sector during 2025 and 2026 (upto June) respectively.

viii. The Cyber Security Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet by CERT-In in April 2022 are in force. Under these directions, CERT-In's cyber incident reporting mandate requires corporate entities to notify CERT-In within six hours of noticing an incident.
ix. CERT-In has conducted 3 cyber security exercises for the Power Sector in 2025 to enable assessment of preparedness to deal with cyber attacks, wherein 150 participants from 30 Power sector organizations across utilities, system operators, generation, transmission and distribution entities participated. In the year 2026 (upto June), 2 cyber security Exercises, including one on countering emerging risk due to frontier AI models, were conducted for Power Sector, wherein 274 participants from 103 organizations, participated.

x. The Ministry of Electronics and Information Technology (MeitY) under its various initiatives has supported development of cyber security technology including development of indigenous firewall.

******