GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 528
TO BE ANSWERED ON: 07.02.2025

CYBERATTACK TRENDS AND ENHANCEMENTS IN CYBER RESILIENCE FOR CRITICAL SECTORS

528. SHRI SANJEEV ARORA:

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

(a) The data on cyberattack trends targeting India's critical sectors (e.g., banking, healthcare, energy) over the past five years, including changes in the frequency and sophistication of attacks; and
(b) The Ministry's plans to enhance cyber resilience through a multi-layered security approach, specifically including AI-driven threat detection, national cybersecurity testing centres, and real-time incident reporting mechanisms?

ANSWER

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

(a) and (b): The policies of the Government are aimed at ensuring an open, safe,trusted and accountable internet for its users. 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.

As per the information reported to and tracked by CERT-In, the total number of cyber security incidents in the last five years are given below:

Year	Number of cyber security incidents
2020	11,58,208
2021	14,02,809
2022	13,91,457
2023	15,92,917
2024	20,41,360

The following measures have been taken for sharing alerts with organisations across sectors:

i. Technical training sessions in the area of AI-powered cybersecurity threats and Internet of Things (IoT) security were conducted by Indian Computer Emergency Response Team (CERT-In) with experts from industry to help the participants understand the latest threat landscape and best practices.
ii. CERT-In is operating an automated cyber threat intelligence exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
iii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.

iv. CERT-In has empanelled 191 security auditing organisations to support and audit implementation of Information Security Best Practices.

v. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

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 formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors to enable the organisations to deal with cyber-attacks and enhance resilience.

viii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 108 such drills have so far been conducted by CERT-In where 1,435 organizations from different states and sectors participated.

ix. CERT-In 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 andtrusted internet.

x. CERT-In has issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024. SBOM helps organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

xi. 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.

xii. CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

xiii. CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers (CISO) of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. A total of 12,014 officials have been trained in 23 training programs in 2024.

****