GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 1338
TO BE ANSWERED ON: 06.12.2024

PLANS TO ENHANCE CYBER RESILIENCE

1338. SHRI SANJEEV ARORA:

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

(a) the total number of cybersecurity incidents reported in the country over the past three years, including data on attacks on critical infrastructure such as health, banking, defence and energy sectors;
(b) the manner in which Government plans to enhance cyber resilience at the national level, particularly through the development of national cybersecurity standards, training of personnel and collaboration with international agencies; and
(c) the efforts made by Government to promote cyber hygiene awareness among citizens, particularly in relation to online fraud, identity theft and phishing attacks?

ANSWER

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

(a): The Government is committed to ensure that the Internet in India is Open, Safe, Trusted and Accountable 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 Indian Computer Emergency Response Team (CERT-In), total number of 1402809, 1391457 and 1592917 cyber security incidents are observed during the year 2021, 2022 and 2023 respectively.

(b) and (c): The Government is fully cognizant and aware of enhancing cyber resilience at the national level, especially as digital threats continue to evolve globally. To strengthen the nation's cybersecurity posture and ensure the protection of critical infrastructure, businesses and citizens, the Government has taken several key initiatives which, inter alia, includes:

i. Government has given directions to all Central Ministries/Departments and States/UTs to appoint Chief Information Security Officers (CISOs) to deal with cyber security matters.
ii. The Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country under the provisions of section 70A of the Information Technology (IT) Act, 2000.
iii. National Informatics Centre (NIC) provides IT support to ministries, departments and agencies of the Central Government, State Governments and district administrators for various e-governance solutions and follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber attacks and safeguarding data.
iv. 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.
v. 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 & Trusted Internet.

vi. CERT-In 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.

vii. CERT-In 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 to help organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

viii. CERT-In issued an advisory to various Ministries in November 2023 outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.

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.

x. CERT-In operates 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.

xi. CERT-In has empanelled 155 security auditing organisations to support and audit implementation of Information Security Best Practices.

xii. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors.

xiii. CERT-In collaborates with Industry to exchange information on latest cyber threats, best practices, and conduct joint skilling and capacity building programs.

xiv. CERT-In coordinates incident response measures with international CERTs, service providers as well as law enforcement agencies.

xv. CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government, public and private sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks.

xvi. CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

xvii. The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Books, videos and online materials about information security are developed for general users, children and parents, and are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

****