GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1340
TO BE ANSWERED ON: 06.12.2024

CYBER ATTACKS ON GOVERNMENT ENTITIES AND DEPARTMENTS

1340. SMT. RENUKA CHOWDHURY:

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

(a) whether it is a fact that many Government entities and departments, including defence units, experienced cyber attacks in recent times, if so, the number of such attacks reported over the last five years;
(b) the economic loss incurred by Government due to these attacks over the last five years, including the cost of securing the online platforms; and
(c) the steps taken by Government in response to the increasing frequency of such attacks on Government entities and departments?

ANSWER

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

(a) to (c): The policies of the Government are aimed at ensuring an Open, Safe and 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 Indian Computer Emergency Response Team (CERT-In), the total number of cyber security incidents pertaining to Government organizations are given below:

Year	Number of cyber security incidents pertaining to Government organizations
2019	85797
2020	54314
2021	48285
2022	192439
2023	204844

Government is fully cognizant and aware of various cyber security threats and has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

(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.) NCIIPC provides threat intelligence, situational awareness, alerts & advisories and information on vulnerabilities to organisations having Critical Information Infrastructure (Clls)/ Protected Systems (PSs) for taking preventive measures from cyber attacks and cyber terrorism.

(iv.) 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.

(v.) 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.

(vi.) 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, and also provides cyber security tips and best practices for citizens and organisations.

(vii.) The Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) has been setup for responding to and containing and mitigating cyber security incidents reported from the financial sector under the umbrella and guidance of CERT-In.

(viii.) 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.

(ix.) 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.

(x.) 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.

(xi.) 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.

(xii.) 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.

(xiii.) 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.

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

(xv.) CERT-In coordinates incident response measures with international CERTs, service providers as well as Law Enforcement Agencies (LEAs).

(xvi.) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations and enhance resilience in Government and critical sectors.

(xvii.) National Informatics Centre (NIC) provides Information Technology (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.

****