GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 541
TO BE ANSWERED ON: 20.07.2022

CYBER ATTACKS

541. SHRIMATI SARMISTHA SETHI:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a)whether the critical infrastructure in the country involving gas-water supply and security installations are at risk of cyber-attacks;
(b) if so, the details thereof including the number of cyber attacks reported in the country;
(c)whether the Government is planning cybersecurity training programme for the Government employees;
(d) if so, the details thereof; and
(e) the other steps taken/being taken by the Government to prevent the cyber attacks in the country?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. The Government via National Critical Information Infrastructure Protection Centre (NCIIPC) is aware of all Critical Information Infrastructure (CII) that require protection. Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India.

(b): CERT-In has reported that a total number of 14,02,809 & 6,74,021 cyber security incidents are observed during the year 2021 & 2022 (upto June) respectively.

(c) and (d): Government has taken following training initiatives which, inter alia, include:

i. Ministry of Electronics and Information Technology (MeitY) has implemented 'Information Security Education and Awareness' (ISEA) programme with the objective of capacity building in the area of Information Security, training of Government personnel and creation of mass Information Security awareness. The project is implemented with 52 academic and training institutions across the country through formal and non-formal courses.

Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through portals like “www.infosecawareness.in”, and “www.cyberswachhtakendra.gov.in”.

ii. MeitYoffers generic training (awareness level) and foundation training (advanced level) online in Cyber Security for officers of Central Government Ministries/Departments. A total number of 10700 officers/staff from various Ministries/Departments have attended generic training (awareness level) and 605 officers/staff have attended foundation training (advanced level).

iii. MeitY conducts deep dive training on cyber security for Chief Information Security Officers (CISOs) and frontline IT officials from Central/State Governments, Public Sector Undertakings (PSUs), PSU Banks and Government organisations in collaboration with industry consortium in Public Private Partnership (PPP) mode to enable them to deal with challenges of cyber security.

iv. Indian Computer Emergency Response Team (CERT-In) conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 19 and 5 training programs were conducted covering 5169 and 449 participants during the year 2021 and 2022 (upto June) respectively.

v. Cyber security exercises and drills are conducted regularly by CERT-In for capacity building and to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 67 such drills have so far been conducted by CERT-In where 886 organizations from different states and sectors participated.

vi. CERT-In conducts workshops for Ministries, Departments, States & UTs and organizations to sensitise them about the cyber security threat landscape and enable them to prepare and implement the Cyber Crisis Management Plan (CCMP). 134 CCMP workshops were conducted till June 2022 by CERT-In.

vii. The cyber-security training programmes for employees of Government and Private Sector Utilities in the Power Sector are conducted through the designated Institutes like National Power Training Institute (NPTI).

viii. Cyber security training besides awareness programs and sessions are conducted regularly for all Information Technology (IT) / Operational Technology (OT) personnel of Power Sector Utilities and other stake holders.

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

i. Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies.

ii. Security tips are published by CERT-In for users to secure their desktops, mobile/smart phones and preventing phishing attacks.

iii. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

iv. 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.

v. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

vi. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

vii. CERT-In also co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies

viii. The analytic centre at National Critical Information Infrastructure Protection Center (NCIIPC) provides near real time threat intelligence and situational awareness based on which regular alerts and tailored advisories are sent to Critical Information Infrastructure/ Protected System entities .

****