GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 5701
TO BE ANSWERED ON: 06.04.2022

CYBER SECURITY

5701. SHRI BENNY BEHANAN:

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

(a) whether the Government is aware of the fact that over 62 per cent of Indian small and medium businesses that participated in a study by CISCO, reported to have lost more than Rs.3.5 crores last year due to cyber attacks;

(b) if so, the details of the steps taken by the Government to help domestic businesses to strengthen their cybersecurity;

(c) whether the Government is aware that the annual report by the US-China Economic and Security Review Commission (USCC) found an increase in cyber attacks from Chinese organisations targeting India;

(d) if so, whether the Government investigated aforesaid claims; and

(e) if so, the details thereof including the efforts made by the Government to strengthen cyber security from such attacks and if not, the reasons therefor?

ANSWER

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

(a) and (b): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. There are media articles, citing a report published by CISCO, stating that over 62 per cent of Indian small and medium businesses that participated in a study by CISCO, reported to have lost more than Rs.3.5 crores last year due to cyber attacks. The findings of such reports by the company are generally based on data generated by their products or survey of their customers. The details of such data is not available and hence cannot be verified.

(c) and (d): There have been media reports about increase in cyber attacks from Chinese organisations targeting India. Government is aware of the fact that there are attempts from time to time to launch cyber-attacks on Indian cyber space. Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. According to the analysis by Indian Computer Emergency Response Team (CERT-In), the Internet Protocol (IP) addresses of the computers from where the attacks appear to be originated belong to various countries including Algeria, Brazil, China, France, Germany, Hong Kong, Indonesia, Netherlands, North Korea, Pakistan, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, Turkey, USA, Vietnam etc.

(e): Government is fully cognizant and aware of various cyber security threats and has taken measures to enhance the cyber security posture and prevent cyber security incidents, which inter alia, include:

(i). The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

(ii). CERT-In operates an automated cyber threat exchange platform for proactively collection, analysis and sharing of tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(iii). The Government has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State/UT Governments and their organizations and critical sectors.

(iv). CERT-In regularly conducts workshops for Ministries, Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape. This enables them to prepare and implement the Cyber Crisis Management Plan. A total of 128 workshops were conducted so far, out of these 31 CCMP workshops were conducted during the year 2021.

(v). Cyber security mock drills are conducted regularly in Government and critical sectors. 64 such drills have so far been conducted by CERT-In where 820 organisations from different States and sectors participated.

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

(vii). All the government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

(viii). CERT-In has empanelled 96 security auditing organisations to support and audit implementation of Information Security Best Practices.

(ix). 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. 15 and 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 respectively.

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

(xi). CERT-In provides the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

(xii). 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.

(xiii). Ministry of Electronics & Information Technology (MeitY) conducts programs to generate information security awareness. Specific books, videos and online materials are are disseminated through portals like “www.infosecawareness.in”, and “www.csk.gov.in”.

****