GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.1382
TO BE ANSWERED ON: 19.12.2018

CYBER ATTACKS

1382. SHRI OM BIRLA:
SHRI RAM KUMAR SHARMA:

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

(a) whether the Government has taken note of the fact that incidents of cyber attacks including ransomware etc. have increased in the recent past;
(b) if so, the details thereof for the last one year including the measures taken by the Government in this regard;
(c) whether foreign Governments are behind any such cyber attacks, if so, the details thereof and the effective steps taken by the Government in this regard; and
(d) whether lack of trained professionals is proving to be an impediment in curbing such challenges, if so, the reasons therefor and the steps taken by the Government to augment the capacity of existing experts and for training of new experts?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a) and (b): With the proliferation of Information Technology and related services, there is a rise in cyber attacks in the country like elsewhere in the world. Cyberspace is virtual and borderless, thus cyber attacks can come from anywhere, anytime and by anyone. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 53081 cyber security incidents including 56 ransomware incidents were observed during the year 2017.

(c): Cyber attacks by foreign countries are a global phenomenon. The virtual, borderless and anonymous nature of cyberspace provides opportunity to anyone to carry out such cyber attacks. There have been attempts from time-to-time to launch cyber attacks on Indian cyber space. These attacks have been observed to be originating from the cyber space of a number of countries. It has been observed that the attackers compromise computer systems located in different parts of the World and use masquerading techniques and hidden servers to hide the identity of actual system from which the attacks are being launched.

Government has taken a number of legal, technical and administrative measures to address the issue of cyber attacks. These *inter alia*, include:

(i) Information Technology Act, 2000 was enacted to deal with cyber crime. IT Act has adequate deterrent provisions for cyber threats and cyber attacks.

(ii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the IT Act, 2000 for protection of critical information infrastructure in the country.

(iii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in).

(iv) Government has set up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has already been made operational.

(v) Government has launched 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 for banks as well as common users.

(vi) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 38 such exercises have so far been conducted by CERT-In wherein organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc. participated.

(vii) Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices. 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.

(viii) Ministry of Home Affairs (MHA) has launched a portal www.cybercrime.gov.in for public to report complaints of child pornography and sexually abusive explicit content.

(d): Cyber security is a challenging field because of ever changing threat scenario. Ministry of Electronics & Information Technology (MeitY) has initiated Information Security Education and Awareness (ISEA) Project for capacity building in the area of cyber security. ISEA Project Phase II was approved in the year 2014 with an objective of capacity building in the area of Information Security, training of Government personnel and creation of mass Information Security awareness targeted towards various user segments. The project aims to train more than 1 lakh candidates in various formal/non-formal courses and more than 13,000 Government officials by March 2020. In addition, the project envisages creation of mass awareness on Information Security through direct and indirect mode.

So far, 37,018 candidates have been trained/under-going training in various formal/non-formal courses through 52 institutions and 6,042Government officials have been trained in various short term courses of 2/3/5 days duration in the area of Information Security. Besides this, 760 half day general awareness workshops on Information Security have been organized across the country for various user groups covering 82,328 participants. Information Security Awareness handbooks were distributed as a part of these workshops to disseminate information and tips on safe use of internet including ransomware. The softcopy of the

handbook and awareness videos on ransomware are also made available for download on the website www.isea.gov.in.

CERT-In is conducting 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. 22 trainings covering 746 participants conducted in the year 2018 (till November).

****