GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 588
TO BE ANSWERED ON: 19.07.2017

CYBER ATTACK

588 SHRI JITENDRA CHAUDHURY: SHRI DHARAM VIRA: SHRI HARISH MEENA: SHRI KUNWAR PUSHPENDRA SINGH CHANDEL: SHRI RAJU SHETTY: SHRI R. DHRUVA NARAYANA:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a) whether recently there was a world-wide cyber attack including India;
(b) if so, the details thereof and the damages caused as a result thereof;
(c) the steps being taken by the Government in this regard;
(d) whether any study has been conducted to identify the cyber threats in the country and if so, the details thereof;
(e) whether adequate number of cyber security experts are available in the country and if so, the steps being taken in this regard; and
(f) whether Government is planning to amend the existing regulations for promotion of cyber security and if so, the steps being taken in this regard, so far?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a) and (b): Propagation of ransomware called WannaCry / WannaCrypt has been reported in many countries around the world including India since 12 May 2017. Propagation of another ransomware called Petya was also reported since 27 June 2017. Ransomware is a type of malicious software that infects a computer and restricts users' access to affected files by encrypting them until a ransom is paid to unlock it.
34 incidents have been reported to the Indian Computer Emergency Response Team (CERT-In) from organisations and individuals regarding infections of Wannacry and Petya ransomware. As reported to CERT-In, operations of one sea port were partially affected by the Petya ransomware. Remedial measures to contain damage and prevent such incidents have been advised by CERT-In.

(c): The following steps have been taken by the Government to prevent recent ransomware attacks, namely:-
i. CERT-In has issued an advisory regarding detection and prevention of Wannacry ransomware on its website on 13 May 2017. Advisory regarding detection and prevention of Petya ransomware was issued by CERT-In on 27 June 2017.
ii. CERT-In has issued a vulnerability note on its website with a Severity Rating of 'High' on March 15, 2017 suggesting information regarding vulnerabilities in Microsoft Windows systems which have been exploited by Wannacry ransomware alongwith remedial measures.
iii. CERT-In has informed various key oragnisations in the country regarding the ransomware threat and advised measures to be taken to prevent the same. A webcast was also conducted in this regard for organisations and users.

iv. Free tools for detection and removal of wannacry ransomware have been provided on the website of Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in).

Apart from the specific steps mentioned above, the following steps have also been taken to prevent malware/ransomware threats, namely:-

i. The CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect systems and mobile devices.
ii. 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.
iii. Security tips have been published for users to secure their Desktops and mobile/smart phones.
iv. Ministry of Electronics & Information Technology (MEITY) regularly conducts programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like "http://infosecawareness.in/" and www.cyberswachhtakendra.in

(d): In tune with the dynamic nature of Information Technology and limited time available for an effective response, continuous efforts are required to be made to detect and prevent cyber attacks by way of continuous threat assessment and near real-time situational awareness. Such timely information enables coordinated actions by the stakeholders to take appropriate proactive and preventive actions.

Concerted efforts are being made to harvest the requisite information from multiple sources. These include incidents reported to and tracked by CERT-In, technical measures, security cooperation arrangement with overseas Computer Emergency Response Teams (CERTs) and leading security product and service vendors as well as agencies within the government. In addition, the study reports published by various agencies across the world are also studied to understand the historical data with respect to global threat landscape and threat predictions. As such, Government has not conducted a separate study to identify cyber threats.

(e): Towards enhancing qualified cyber security manpower, following steps have been taken, namely:-

i. Ministry of Electronics and Information Technology is implementing the Information Security Education and Awareness (ISEA) project which aims to generate 1.14 lakhs qualified professionals at various levels in period of 5 years. A total of 52 institutions in various categories across the country are participating in the project. Besides, National Institute of Electronics and Information Technology (NIELIT) is conducting certification courses for creation of cyber security professionals.
ii. CERT-In conducts regular training programme to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber attacks. CERT-In is regularly conducting Cyber Crisis Management Plan (CCMP) workshops for Central Government Ministries/Departments, States & UTs and critical sector organisations to sensitise them about the cyber security threat landscape, enabling them to prepare and implement the Cyber Crisis Management Plan as well as participate in the mock drill exercises.
iii. Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI), Ghaziabad to impart basic and advanced training in cyber forensics and investigation of cybercrimes to police officers. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.
iv. Data Security Council of India (DSCI), NASSCOM and Cyber Forensic Labs set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime

investigation. Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

v. NASSCOM & DSCI have been working under the aegis of National Skill Development Corporation, Ministry of Skill Development and Entrepreneurship, on developing standardized content for the key job roles that have been identified based on the industry inputs, requirements and response.

(f):Presently there is no proposal with the Government to amend the Information Technology Act, 2000.

****