GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3652
TO BE ANSWERED ON: 07.12.2016

CYBER SECURITY

3652 DR. GOKARAJU GANGA RAJU:
SHRI PRATHAP SIMHA:
KUMARI SHOBHA KARANDLAJE:
SHRI BAIJAYANT JAY PANDA:

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

(a) whether there is steady increase of internet created cyber security risks;
(b) if so, the details thereof and Government/private reports received in this regard along with the reaction of the Government thereto;
(c) whether in India, more and more organisations believe that not all their data stored in the cloud is protected;
(d) if so, the details thereof; and
(e) the corrective measures being taken by the Government to adopt next-gen security to minimise cyber threats to transform and upgrade security strategy and systems to ensure the safekeeping of all data?

ANSWER

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

(a) and (b): The area of Information Technology (IT) is characterized by rapid developments and dynamic growth. With every IT product and service introduced into the market, newer vulnerabilities are discovered, leaving scope for malicious actions. Over a period, the nature and pattern of incidents have become more sophisticated and complex. In tune with the dynamic nature of Information Technology and limited time window available for an effective response, continuous efforts are required to be made to detect and prevent cyber attacks and ensuring safekeeping of data.

With the proliferation of Information Technology, Internet users and related services, there is a rise in number of cyber security incidents in the country as elsewhere in the world. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 44679, 49455 and 39730 cyber security incidents were observed during the year 2014, 2015 and 2016 (till October) respectively showing a steady increase. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, Denial of Service attacks, etc.

Government has not received any Government/private reports in this regard.

(c) and (d): Government has not conducted any study/assessment in this regard. However, Government understands the need for security of data stored in cloud. Ministry of Electronics and Information Technology in its “Request For Proposal (RFP) for Provisional Empanelment of Cloud Service offerings of Cloud Service Providers” has addressed specific requirement for cloud security.

(e) : Government has taken the following steps to prevent data theft and enhance cyber security:

i. 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). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out.

ii. Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, States /UT Governments and their organizations and critical sectors. The Crisis Management Plan is updated periodically on annual basis to take into account changing scenario of cyber threat landscape. Regular workshops are conducted for Ministries, Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan. So far 41 workshops have been conducted.

iii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 11 such drills have so far been conducted by CERT-In where 110 organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space and IT/ITeS participated.

iv. Government has empaneled security auditing organisations to support and audit implementation of Information Security Best Practices. Currently, 57 organisations have been empaneled.

v. Operationalising the National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology Act 2000, for protection of Critical Information Infrastructure in the country. NCIIPC is providing tailored advisories on software/hardware vulnerabilities and alerts on cyber attacks are being issued regularly to Chief Information Security Officers of Critical Information Infrastructure organizations. In addition policy, audit and compliance reports of Critical Information Infrastructure organizations are being analysed.

vi. Government is establishing Botnet cleaning and malware analysis centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.

i. Government is setting 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.

ii. Government is implementing 'Information Security Education and Awareness (ISEA)’ project to train professionals / government officials and create mass information security awareness among citizens. The Project is implemented by 51 institutions across the country. So far, 11,110 persons have been trained/undergoing training in various formal/non-formal courses focusing on Cyber Security. 2,384 Government personnel have been trained in direct training programs. C-DAC Hyderabad has conducted 377 Awareness workshops for various user groups covering 42,379 participants from 22 States/UT.

iii. CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. As on 31st October, 14 such training programs have been conducted covering 431 participants during the year 2016.

iv. Government has set up cyber forensic training & investigation labs for training of officers of Law Enforcement agencies and Judiciary. More than 1250 police officers in North Eastern states have been trained. In addition, National Institute of Technical Teachers Training and Research(NITTTR), Chandigarh has trained 2756 Engineering and Polytechnic college teachers, whereas National Law School of India University (NLSIU), Bangalore imparted training to 1398 officials including judiciary, law teachers & practitioners, law students, law researchers, etc.

****