GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2632
TO BE ANSWERED ON: 24.03.2017

INCREASE IN CYBER SECURITY THREATS

2632. SHRI PREM CHAND GUPTA:
SHRI SURENDRA SINGH NAGAR:

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

(a) whether cyber security threat due to internet has increased continuously;
(b) if so, the details thereof and the details of Government/non-Government reports in this regard and the reaction of Government thereto;
(c) whether most organisations in the country have begun to believe that all their information gathered through cloud systems is not safe, if so, the details thereof; and
(d) the remedial steps being taken by Government to ensure safety of all kinds of information, adopt higher security systems to minimize cyber threats and transform and upgrade safety strategies and mechanism?

ANSWER

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

(a) and (b): With the proliferation of Information Technology and related services there is a rise in number of cyber security incidents in the country like elsewhere in the world. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455 and 50362 cyber security incidents were observed during the year 2014, 2015 and 2016 respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, Denial of Service attacks, etc. Over a period, the nature and pattern of incidents are becoming more sophisticated and complex. In tune with the dynamic nature of Information Technology continuous efforts are required to be made to detect and prevent cyber attacks.

(c): There is no such study conducted by the Government.

(d): Government has taken a number of legal, technical and administrative policy measures for addressing cyber security. This includes National Cyber Security policy (2013), Framework for enhancing Cyber Security (2013), enactment of Information Technology (IT) Act, 2000 and setting up of Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT Act, 2000.

(i) The Information Technology (IT) Act, 2000 has adequate provisions for safety of sensitive personal information.
(ii) Government is implementing a Framework for enhancing cyber security, with a multi-layered approach for ensuring defence-in-depth and clear demarcation of responsibilities among the stakeholder organizations in the country.

(iii) 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.

(iv) 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.

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

(vi) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

(vii) Government has initiated setting up of 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.

(viii) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.

(ix) 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 and Judiciary in these States.

(x) Industry associations such as Data Security Council of India (DSCI), NASSCOM, 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.

(xi) A number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed indigenously and such tools are being used by Law Enforcement Agencies.

(xii) CERT-In and Centre for Development of Advanced Computing (C-DAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

(xiii) Reserve Bank of India (RBI) issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI also issues advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds.

(xiv) All banks have been mandated to report cyber security incidents to CERT-In expeditiously.

(xv) All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised to carry out audit by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In) on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices. CERT-In has empaneled 32 security auditing organisations to support and audit implementation of Information Security Best Practices.

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

(xvii) 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.

(xviii) Ministry of Home Affairs has issued National Information Security Policy and Guidelines (NISPG) to Government organizations to ensure safety of data and minimize cyber threats.

****