GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
QUESTION NO 2957
ANSWERED ON 11.08.2017

Increase in cyber crimes

2957 Smt. Ambika Soni

Dr. T. Subbarami Reddy

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

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

(a) whether cases of cyber crime are increasing year by year, if so, the details thereof, year-wise for last five years;
(b) the concrete steps being taken or proposed to be taken to place critical infrastructure to predict and prevent cyber crimes like phishing, site intrusions, defacements, virus or malicious code, ransomware, etc.;
(c) whether the present IT laws are adequate to deal with the growing cyber and virus attacks; and
(d) if not, the measures to be taken by Government to ensure safety and security of software programmes and networking in the country?

ANSWER

(a): With the proliferation of Information Technology and related services, there is a rise in instances of cyber crimes in the country like elsewhere in the world. As per the data maintained by National Crime Records Bureau (NCRB), a total of 4356, 7201, 9622, 11592 and 12317 cyber crime cases were registered during the years 2012, 2013, 2014, 2015 and 2016 respectively. This includes cases registered under the Information Technology (IT) Act, 2000 and related sections of Indian Penal Code and Special & Local Laws involving computer as medium/ target.

(b): Government has taken a number of legal, technical and administrative measures for addressing cyber security. These inter alia, include the following:

(i) Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for dealing with prevalent cyber crimes.
(ii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology (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 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. Phase-I of NCCC has been made operational.
(v) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.
(vi) 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.

(vii) A number of Cyber forensics tools for collection, analysis and presentation of the digital evidence have been developed indigenously and such tools are being used by law enforcement agencies.
(viii) 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.
(ix) All banks have been mandated to report cyber security incidents to CERT-In expeditiously.
(x) All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised to carry out audit by the empanelled auditors of 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. Government has empanelled 54 security auditing organisations to support and audit implementation of Information Security Best Practices.
(xi) 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.
(xii) 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.
(xiii) 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.
(xiv) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different states and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc have participated.

(c) and (d): The Information Technology Act, 2000 provides adequate legal framework to deal with the prevalent cyber security breaches.

****