GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 244
TO BE ANSWERED ON: 03.02.2017

INCREASE IN CYBER CRIMES

244 SHRI VIVEK GUPTA:

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

(a) whether it is a fact that the number of cyber crime cases in the country have increased four-fold in the last three years;

(b) Whether Government has any mechanism to guide and fund State Government to ensure security of digital Government data, if so, the details thereof;

(c) The details of steps Government has taken to guard against external cyber attacks; and

(d) The details of money spent over past three years, State-wise, for improving the cyber security?

ANSWER

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

(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.

(i). As per the data maintained by National Crime Records Bureau (NCRB), a total of 5693, 9622 and 11592 cyber crime cases were registered during the years 2013, 2014 and 2015 respectively.

(ii). RBI has registered a total of 9500, 13083, 16468, and 8689 cases of frauds involving credit cards, ATM / debit cards and internet banking during the year 2013-14, 2014-15, 2015-16 and 2016-17(upto December 2016), respectively.

(iii). CBI has registered a total of 93 cases during 2013–2016 under Information Technology (IT) Act, 2000.

(iv). 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 including phishing, scanning, malicious code, website intrusion, Denial of Service etc., were reported during the year 2014, 2015 and 2016 respectively.

(b): Ministry of Electronics & Information Technology (MeitY) has well defined system/ guidelines to support/fund State/UT Governments for their e-Governance initiatives under the Digital India programme. The security of the overall system developed is an integral component of such e-Governance projects.

(c): Government has taken various steps in the form of legal framework, emergency response, awareness, training, and implementation of best practices to guard against external cyber-attacks. Such steps include:

(i). The Information Technology (IT) Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

(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 Information Technology Act, 2000 for protection of Critical Information Infrastructure in the country.

(iv). With respect to the banking sector, in order to focus more attention on IT related matters, Reserve Bank of India has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015. The Bank has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security. The circular requires banks to have among other things, a cyber-security policy, cyber crisis management plan, a gap assessment vis-à-vis the baseline requirements indicated in the circular, monitoring certain risk indicators in the area, report unusual cyber security incidents within 2 to 6 hours, ensure board involvement in the matter and robust vendor risk management. The progress of banks in scaling up their cyber security preparedness is monitored.

(v). RBI carries out IT Examination of banks separately from the regular financial examination of banks from last year. This report has a special focus on cyber security. The reports have been issued to the banks for remedial action. RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents. Department of Banking Supervision also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In. RBI also has set up an IT subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities. The subsidiary is in the process of recruiting the experts.

(vi). CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has issued 372, 402 and 432 advisories during 2014, 2015 and 2016 respectively. 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.

(vii). 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.

(viii). 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, Spaces and IT/ITeS participated.

(ix). Government has established 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.

(x). 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.

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

(xii). 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.

(xiii). 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. In academia National Law School, Bangalore and NALSAR University of Law, Hyderabad is also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

(xiv). 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.

(xv). CERT-In and Centre for Development of Advanced Computing (C-DAC) are 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.

(xvi). Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States.

(xvii). 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.

(xviii). 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. 11,110 persons have been trained/undergoing training in various formal/non-formal courses focusing on Cyber Security till 2016. Through direct training programs 2,384 Government personnel have been trained. C-DAC Hyderabad has conducted 377 Awareness workshops for various user groups covering 42,379 participants from 22 States/UT till 2016.

(xix). CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 18 such training programs were conducted covering 580 participants during the year 2016. In addition a workshop on security of digital payments systems has been conducted for stakeholder organisations covering 110 participants.

(xx). Currently 24 security auditing organizations are empanelled to support and audit implementation of Information Security Best Practices.

(xxi). NIC protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place. NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems and anti-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardening. These are complemented by round-the-clock monitoring of security events and remedial measures are carried out for solving the problems subsequently. A 24x7 security monitoring centre is in place at NIC for detecting and responding to security incidents. Restoration is done after detected incident is analysed and necessary remedial measures are taken.

(d): Rs. 500 Crores has been allocated for Ministry of Electronics and Information Technology (MeitY) in the 12th Plan period (2012-17) for Cyber Security Programme including Cyber Safety, Security and Surveillance, Cyber Crime Investigations and Cyber Forensics.

****