GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:4026
ANSWERED ON:19.02.2014
CYBER FRAUDS
Dhruvanarayana Shri R. ;Mahendrasinh Shri Chauhan ;Rathwa Shri Ramsinhbhai Patalbhai;Siricilla Shri Rajaiah

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

-

(a) the number of cases of cyber frauds reported in the country during the last three years and the current year;

(b) whether the existing laws are capable to deal with cyber criminals and punish them adequately;

(c) if so, the details thereof and the action taken by the Government to prevent cyber frauds;

(d) whether a large number of information technology experts are migrating to foreign countries every year; and

(e) if so, the reasons therefor and the action taken by the Government to generate employment opportunities for the information technology experts in the country?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY
(SHRI MILIND DEORA)

(a): Police and Public Order are State subjects under the Constitution and as such the State Governments and Union Territory Administrations are primarily responsible for prevention, detection, registration and investigation of crime including Cyber Frauds and for prosecuting the criminals through Law Enforcement machinery within their jurisdictions.

As per the cyber crime data maintained by National Crime Records Bureau, a total of 966, 1791 and 2876 Cyber Crime cases were registered under Information Technology Act during 2010, 2011 and 2012 respectively. A total of 356, 422 and 601 cases were registered under Cyber Crime related Sections of Indian Penal Court (IPC) during 2010, 2011 and 2012 respectively. As per the information provided by Reserve Bank of India (RBI), 14271, 10048, 8765 and 6034 cyber fraud cases have been reported to the RBI during 2010-11, 2011-12, 2012-13 and 2013-14 (up to 30-09-2013) respectively. Central Bureau of Investigation (CBI) has registered 12, 11 and 11 cases during 2011, 2012 and 2013 (up to 30-11-2013) respectively.

(b) and (c): The Information Technology Act 2000 as amended in 2008 has adequate provisions to deal with prevailing Cyber Crimes. It provides punishment in the form of imprisonment ranging from two years to life imprisonment and fine / penalty depending on the type of Cyber Crime.

Government has taken a series of measures covering aspects like legal, technical and administrative to address the growing incidents of Cyber crimes in the country. The steps include:

Reserve Bank of India (RBI) has issued a Circular to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI has also advised Banks to leverage technology to support Business processes and implement all stipulations outlined by RBI from time tc time. Banks are also advised to ensure implementation of basic Organizational framework and put in place policy and procedures to prevent financial frauds through Internet.

Reserve Bank of India (RBI) has issued several advisories on Credit Card operations by Banks. Use of PIN has been made mandatory in the transactions. The Banks have been advised to set up internal control system to combat frauds and to take proactive fraud control and enforcement measures. The Banks are required to fulfill `Know Your Customer (KYC)` requirements. RBI has also issued advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds. RBI also has cautioned public through Notification against fictitious offers of remitting cheap funds from abroad.

Ministry of Home Affairs has issued an Advisory to the State Governments and Union Territory Administrations to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes. Also, under the Cyber Crime Investigation programme, Ministry of Home Affairs is supporting the establishment of Cyber Crime Police Stations (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each State / Union Territory of India under Police Modernization Scheme. Action also has been taken to set up a National Centre of Excellence exclusively devoted to render Cyber Forensic services and to act as National Research and Training Centre on Cyber Forensics.

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.

A major programme has been initiated on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyze the digital evidence and present them in Courts.

Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) 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.

Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. 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 and Judiciary in these States.

In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. 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.

Indian Computer Emergency Response Team (CERT-In) issues alerts, advisories and guidelines regarding cyber security threats and measures to be taken to prevent cyber incidents and enhance security of Information Technology systems.

(d) and (e): The Information Technology Industry is dynamic, vibrant and market driven. The Information Technology experts are highly mobile based on the opportunities available to them across the globe including India to implement and deliver Information Technology projects. Information Technology industry is executing large number of projects for their clients abroad from India. More or less all Information Technology companies of world have established their development centre in India. It has helped in retaining manpower in India. The country is further focusing on skill development. Government has been regularly creating opportunities through key Information Technology flagship projects in the area of e-Governance, State Data Centres, Aadhaar etc. Government has also established Centres of Excellance like Information Technology Research Academy (ITRA), Media Lab Asia, Centre for Development of Advanced Computing (CDAC), Centre for Development of Telematics (CDOT) to attract best talent in the Information Technology field.