

**GOVERNMENT OF INDIA
ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA**

UNSTARRED QUESTION NO:2287

ANSWERED ON:15.03.2017

Global Fraud and Risk Survey

Chavan Shri Ashok Shankarrao;Gaikwad Dr. Sunil Baliram;Gupta Shri Sudheer;Kirtikar Shri Gajanan Chandrakant;Radhakrishnan Shri T.;S.R. Shri Vijay Kumar;Singh Shri Kunwar Haribansh

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 according to the 'Global Fraud and Risk Survey for 2016', one out of five top executives of global corporations have expressed their apprehensions over investing in India due to concerns over fraudulent practices and cyber security lapses and if so, the details thereof along with other issues raised in the survey;
- (b) the number of cyber fraud incidents reported during each of the last three years and the current year along with the action taken/being taken by the Government in this regard, State/UT-wise;
- (c) whether there are large number of fake accounts on various e-mail and social networking sites which are being used for committing cyber fraud/crime;
- (d) if so, the details thereof along with the action taken/being taken by the Government in this regard; and
- (e) the corrective measures taken/being taken by the Government on the findings of the Global Fraud and Risk Survey, 2016?

Answer

(a) : There have been media reports based on the 'Global Fraud and Risk Survey for 2016' indicating one out of five top executives of global corporations have expressed their apprehensions over investing in India due to concerns over fraudulent practices and cyber security lapses. However, the report has highlighted reduction in cyber fraud and cyber security incidents cases in past twelve months in India.

(b) and (e) : National Crime Records Bureau (NCRB) collects and maintains statistical data of police recorded cognizable crimes including cyber frauds and cyber crimes from 35 States /Union Territories. As per the data maintained by NCRB, a total of 1600 and 3383 cases were registered under cyber fraud using computer as medium/target during the year 2014 and 2015. Data for the year 2016 is under collection. State/UT-wise data during 2014-2015 is enclosed as Annexure-I.

Government has taken various steps in the form of legal framework, awareness, training, and implementation of best practices to address issues related to cyber crimes including risk identified in the report. These include:

(i) The 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) Ministry of Electronics & Information Technology (MeitY) has recently notified the scheme for evaluating any Department, body or agency of the Central Government or a State Government to notify them as Examiner of Electronic Evidence under section 79A of IT Act, 2000.

(iii) Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has issued 17 advisories since Nov 27, 2016 for security safeguards covering Point of Sale (POS) machines, Micro ATMs, electronic Wallets, online banking, smart phones, Unified Payment Interface (UPI), Unstructured Supplementary Service Data (USSD), RuPay, SIM cards, wireless access points / routers, mobile banking, cloud and Aadhaar Enabled Payment System (AEPS). Advisory has also been sent by CERT-In to RBI, National Payment Corporation of India Limited (NPCIL) and Payment Card Industry Organizations covering precautions to be taken to avoid similar attacks as those that occurred recently with credit / debit cards.

(iv) 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 2 workshops on security of digital payments systems have been conducted for stakeholder organisations covering 110 participants.

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

(vi) With respect to the banking sector, in order to focus more attention on IT related matters, Reserve Bank of India (RBI) has taken various steps which include :

- RBI 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.

36 Puducherry 0 0 0 0 0 0 0 0 0 0

TOTAL UT(S) 68 23 11 12 0 0 124 22 17 19 3 3

TOTAL (ALL INDIA) 1600 555 267 353 4 5 3383 2376 382 633 12 16

Source: Crime in India "" Data Colletion since 2014

Note: The data includes heads "Criminal Breach of Trush+Cheating+Computer Related Offences Section 66D+Create/publish/make available Electronic Signature Certificate for fraudulent/unlawful purpose (Section 74))