GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:3337
ANSWERED ON:16.03.2011
DATA AND TRANSACTION SECURITY
Mirdha Dr. Jyoti

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

(a) whether the Data Security Council of India under CERT-IN has done a survey on the data and transactions security systems in Indian banks;

(b) if so, the findings thereof; and

(c) the action taken/being taken by the Government to ensure security of banking transactions?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI GURUDAS KAMAT)

(a): The Data Security Council of India has done a survey on the 'State of Data Security and Privacy in the Indian Banking Industry' under the aegis of CERT-In in the year 2010 and the report was published in Feb 2011.

(b): Some of the major findings of the survey are summarized as:

(i). Investments in information security are being driven by regulatory requirements as well as the increasing usage of online & mobile channels and external threats.

(ii). Information security is still seen as an IT centric function.

(iii). There is a need for increased synergy between Security and Fraud Management functions.

(iv). Banks face most significant challenges in respect of customer awareness on information security along with insecure customer end points.

(v). Managing security is more challenging in online banking and phone (IVR) banking as compared to other service delivery channels.

(vi). Majority of the banks continue to remain largely dependent on incidents being reported by their customers and/or employees.

(c): Government is following an integrated approach with a series of legal, technical and administrative steps to ensure that necessary systems are in place to address the growing threat of cyber attacks in the country. Salient details are given below:

(i) Computers Security Policies, Standard Operating Procedures and guidelines were formulated and circulated to all Ministries/Departments for implementation.

(ii). All Central Government Ministries/ Departments and State/Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure including websites periodically to discover gaps with respect to security practices and take appropriate corrective actions.

(iii). National Informatics Centre (NIC) has been directed not to host web sites, which are not audited with respect to cyber security.

(iv). The "Crisis Management Plan for countering cyber attacks and cyber terrorism" was prepared and circulated for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

(v). The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with security breaches of information technology infrastructure.

(vi). The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

(vii). Institute of Development & Research in Banking (IDRBT) at Hyderabad has been functioning as a Sectoral CERT in the Finance sector to handle and respond to domain specific threats.

In addition, RBI is regularly advising banks on various aspects related to security of banking transactions.