GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(DEPARTMENT OF ELECTRONICS & INFORMATION TECHNOLOGY)

LOK SABHA

UNSTARRED QUESTION NO. 653

TO BE ANSWERED ON: 02.12.2015

CYBER ATTACK

**653 SHRIMATI RANJEET RANJAN: SHRI SUDHEER GUPTA:
SHRI E.T. MOHAMMED BASHEER: DR. BHOLA SINGH:
DR. SUNIL BALIRAM GAIKWAD: KUNWAR HARIBANSH SINGH:
SHRI NARANBHAI KACHHADIYA: SHRI KAMAL NATH:
SHRI ANOOP MISHRA: SHRI GAJANAN KIRTIKAR:
SHRI LALUBHAI BABUBHAI PATEL: SHRI KANWAR SINGH TANWAR:
SHRI OM BIRLA:**

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

(a) the number of cyber attacks on Indian companies reported in the current financial year;

(b) the reasons for frequent cyber attack on these companies and the losses incurred by these companies as a result thereof;

(c) whether Government has taken any steps to curb cyber attack with rapidly growing interconnected business operations and increasing digitisation and if so, the details thereof; and

(d) whether the Government proposes to amend cyber laws and set up special cyber courts to try cyber cases and if so, the details thereof?

ANSWER

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a): In the current financial year a total number of 54,483 cyber security incidents including phishing, scanning, spam, malicious code, website intrusion/hacking etc., involving Indian cyberspace were reported to the Indian Computer Emergency Response Team (CERT-In). These incidents were reported to CERT-In by various Indian organisations, individuals, CERTs and agencies from other countries.

(b): The area of Information Technology (IT) is characterized by rapid developments and fast changing obsolescence. With every IT product introduced into the market, newer vulnerabilities are discovered, leaving scope for malicious actions. In tune with the dynamic nature of Information Technology, continuous efforts are required to be made to prevent and recover from cyber attacks. Malicious users continuously target India’s IT infrastructure to infiltrate and hamper the functionality of IT systems. As such, the protection of India's IT infrastructure in general and critical information infrastructure in particular is a dynamic activity and continuing process. No separate data with regard to the losses incurred by the Indian companies as a result of cyber attacks is maintained by Indian Computer Emergency Response Team (CERT-In).

(c): The Government has taken the following key steps to curb cyber attacks with rapidly growing interconnected business operations and increasing digitisation and enhance the cyber security of systems in the country:

i. A National Cyber Security Policy has been put in place for public use and implementation by all relevant stakeholders. Its stated mission is "to protect information and information infrastructure in cyber space, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation". It seeks to do so by creating a secure cyber ecosystem and an assurance framework, encouraging open standards, strengthening the regulatory framework, vulnerability management, promotion of research and development in cyber security and enhancing our technical skill sets and human resources.

ii. Efforts towards setting up National Cyber Coordination Centre (NCCC) to generate near real time macroscopic views of the cyber security breaches and cyber security threats in the country. The centre will provide a structured mechanism and facilitate coordination of efforts of all stakeholder agencies in the country. NCCC will be a multi stakeholder body and will be implemented by Indian Computer Emergency Response Team (CERT-In) at Department of Electronics and Information Technology (DeitY).

iii. Efforts towards setting up of “Botnet Cleaning and Malware Analysis Centre” to provide for detection of malware infected computer systems and enable cleaning and securing the systems of end-users to prevent further malware infections. The project is being implemented in coordination and collaboration with Internet Service Providers (ISPs) and Industry. This would help in enhancing the security of computer systems across the country.

iv. Information Technology Act, 2000 provides legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

v. 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.

vi. 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.cert-in.org.in). CERT-In also conducts regular training programme to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber attacks.

vii. Government has setup National Critical Information Infrastructure Protection Centre (NCIIPC) to protect the critical information infrastructure in the country.

viii. All Central Government Ministries / Departments and State / Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure. All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting also. CERT-In provides necessary expertise to audit IT infrastructure of critical and other ICT sectors.

ix. All government websites are to be hosted on infrastructure of National Informatics Centre (NIC), ERNET India or any other secure infrastructure service provider in the country.

x. Sectoral CERTs have been functioning in the areas of Defence and Finance for catering to critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

xi. Information Sharing and Analysis Centres (ISACs) for financial services has been set up at Institute for Development and Research in Banking Technology (IDRBT). Such a centre exchange information on cyber incidents in financial sector and advises them for appropriate mitigation.

xii. The organizations operating critical information infrastructure are regularly advised to implement information security management practices based on International Standard ISO 27001. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems.

xiii. Centres have been setup in the States to train the police officers in area of cyber forensics for investigation of cyber crimes.

xiv. Programmes for creating awareness about cyber security among Government officials and public are continuously being pursued by the government along with organisations from Government and Public.

xv. Cyber Security Mock Drills are being conducted by the Government to help the organisations to assess their preparedness to withstand cyber attacks. Two such drills are being conducted every year with the involvement of organizations.

xvi. The Government is encouraging development of indigenous technology by carrying out Research and Development (R&D) in the area of cyber security.

(d): There is no proposal before the government to amend cyber laws and set up special cyber courts to try cyber cases.

****