GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2504
TO BE ANSWERED ON: 16.03.2018

INCREASE IN CYBER SECURITY RISKS

2504. SHRIMATI JAYA BACHCHAN:

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

(a) whether there is steady increase of internet created cyber security risks;
(b) if so, the details thereof and Government/private reports received in this regard along with the reaction of Government thereto;
(c) whether it is a fact that in India, more and more organisations believe that not all their data stored in the cloud is protected;
(d) if so, the details thereof; and
(e) the corrective measures being taken by Government to adopt next-gen security to minimise cyber threats, to transform and upgrade security strategy and systems to ensure the safekeeping of all data?

ANSWER

MINISTER OFSTATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS)

(a) and (b): With the proliferation of Information Technology and related services there is a rise in number of cyber security incidents *inter-alia* cyber security risk in the country like elsewhere in the world. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455, 50362 and 53081 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, Denial of Service attacks, etc. Over a period, the nature and pattern of incidents are becoming more sophisticated and complex. In tune with the dynamic nature of Information Technology continuous efforts are required to be made to detect and prevent cyber attacks.

(c) and (d): No such study report has come to the notice of the Ministry of Electronics & Information Technology.

(e): Government has taken a number of legal, technical and administrative policy measures for addressing cyber security. These include : (i) National Cyber Security policy, (ii) Framework for enhancing Cyber Security, (iii) enactment of Information Technology (IT) Act, 2000, (iv) setting up of Indian Computer Emergency Response Team (CERT-In), and (v) National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT Act, 2000.

(i) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country. NCIIPC has been regularly advising the critical information infrastructure (CII) sector organisation to reduce vulnerabilities to all kinds of threats and attacks, by sharing threat intelligence, guidelines, best practices and frameworks for protection and guiding them with policies and protection strategies. In addition, training and awareness programs are regularly conducted to improve the cyber hygiene in CII organisations..

(ii) Government has formulated Cyber 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.

(iii) Government has issued general guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(iv) CERT-In has empanelled 67 security auditing organizations to support and audit implementation of Information Security Best Practices.

(v) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

(vi) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 22 training programs covering 610 participants were conducted during the year 2017.

(vii) Government has set up of 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. Phase-I of NCCC has been made operational.

(viii) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

(ix) Government has also directed that all Ministries/Departments and their organisations will earmark 10% of their annual IT budget to implement cyber security for protecting ICT infrastructure.

******