GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 647
TO BE ANSWERED ON: 27.06.2019

PLAN TO TACKLE CYBER ATTACKS

647. SHRI C.M RAMESH:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a) whether Government has initiated any plan to tackle cyber attack incidents of data breaches and some emerging risks likely to affect business environment in the country, and if so the details thereof; and
(b) whether Government proposes to appoint high level committee of experts to study the matter, and to study the safety measures taken by other leading countries of the world in this regard, and if so, the details thereof and if not, the reasons therefor?

ANSWER
MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a) and (b) : In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners to secure data and protect systems and networks by way of hardening and deploying appropriate security controls.

Government is already working on the recommendations including the draft Personal Data Protection Bill submitted by the committee headed by Justice (Retd.) Shri B. N. Srikrishna. The Bill proposes for creation of a Data protection Authority to handle data breaches.
In addition, Government has taken several measures to enhance the cyber security posture and prevent cyber attacks, which *inter alia* includes:
(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis. Regarding securing digital payments, 28 advisories have been issued for users and institutions.Security tips have been published to enable users to secure their Desktops and mobile/smart phones.
(ii) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
(iii) Government has empanelled 84 security auditing organisations to support and audit implementation of Information Security Best Practices.
(iv) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
(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.
(i) Cyber security mock drills and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 43 such exercises have so far been conducted by CERT-In where organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS sectors participated.
(ii) 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. 24 trainings covering 845 participants conducted in the year 2018.
(iii) 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.
(iv) Government has set up 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.

(v) Ministry of Home Affairs (MHA) has launched a portal www.cybercrime.gov.in for public to report complaints of child pornography and sexually abusive explicit content.

****