

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2816
TO BE ANSWERED ON: 10.08.2018

INCIDENTS OF DATA BREACH

2816. SHRI SANJAY SETH:

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

- (a) whether it is a fact that incidents of data breach in the country are higher than the global average;
- (b) if so, the details thereof; and
- (c) the steps Government is taking in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a) and (b): No such authentic report is available with the Government indicating that data breach in the country are higher than the global average.

(c): Government has taken several measures for preventing unauthorised access to data and enhancing the cyber security of information technology infrastructure in the country. These are:

- (i) The Information Technology Act, 2000 has provisions for dealing with data breaches.
- (ii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers/servers on regular basis.
- (iii) 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.
- (iv) Government has empanelled 69 security auditing organisations to support and audit implementation of Information Security Best Practices.
- (v) Government has issued general guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications/infrastructure and compliance.
- (vi) 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.
- (vii) 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. 30 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 etc participated.

- (viii) 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.
