GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.863
TO BE ANSWERED ON: 20.12.2017

RANSOMWARE VIRUS ATTACK

863. SHRI TARIQ ANWAR:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether the Government has conducted any assessment regarding ransomware virus attack and data lost because of it in the country;
(b) if so, the details thereof and if not, the reasons therefor;
(c) the number of cases of virus attack reported across the country so far; and
(d) the steps the Government is considering to save the data of the country from such virus attacks?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ALPHONS KANNANTHANAM)

(a), (b) and (c): As per the information reported to Indian Computer Emergency Response Team (CERT-In), a total no. of 26 and 54 incidents involving ransomware virus were reported during the year 2016 and 2017 (till November) respectively.

(d): The following measures are taken to prevent virus/ransomware attacks and enhance cyber security in the country:

(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and counter measures to protect information systems and mobile devices. Security tips are published for users to secure their Desktops and mobile/smart phones.
(ii) 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 for banks as well as common users.
(iii) 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.
(iv) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 4 such drills have been conducted specifically for ransomware scenarios to enable preparedness of organisations for such threats.
(v) Government has published Guidelines for Chief Information Security Officers (CISOs) for Secure Applications and Infrastructure. Government has also specified key roles and responsibilities of CISOs in Ministries/Departments and Organisations managing ICT operations.
(vi) Ministry of Electronics & Information Technology (MeitY) regularly conducts programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like “http://infosecawareness.in/” and www.cyberswachhtakendra.gov.in.
(vii) National Critical Information Infrastructure Protection Centre (NCIIPC) has been regularly advising the Critical Information Infrastructure (CII) sector organisation to reduce vulnerabilities by sharing threat intelligence, guidelines, best practices and frameworks for protection and also

guiding them with policies and protection strategies. In addition, training and awareness programs are regularly conducted to improve the cyber hygiene in CII organisations.

****