GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1043
TO BE ANSWERED ON: 10.02.2023

CYBER SECURITY ATTACKS

1043. SHRI SUSHIL KUMAR MODI:

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

(a) quantum of data encrypted and number of servers hacked in the recent cyber attack on AIIMS Delhi;
(b) details of cybersecurity lapses found in the conduct of AIIMS Delhi's e-hospital services:
(c) number of cybersecurity incidents reported in the country in the last five years, year-wise;
(d) details of the progress achieved on implementation of the National Cybersecurity Strategy so far; and
(e) whether it includes comprehensive disaster recovery plans for continuation of business activity and Government services post attack, if so, details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The Government is committed to ensure that the Internet in India is Open, Safe and Trusted and Accountable for all its users. With the expansion of the Internet and more and more Indians coming online, the possibility cyber-attacks has also increased. Government is fully cognizant and aware of various cyber security incidents and has taken several measures to enhance the cyber security posture and curb cyber security incidents.
Based on current analysis by concerned stakeholders, five servers of the All India Institute of Medical Sciences (AIIMS), Delhi were affected and approximately 1.3 Tera Bytes of data was encrypted.

(b): The information and computer systems of AIIMS are managed by AIIMS. The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. CERT-In has issued a direction recently making it mandatory for all incidents to be mandatorily reported to CERT-In. Upon receipt of information about occurrence of a cyber security incident from AIIMS, CERT-In carried out an evaluation of the incident. As per the analysis, servers in the information technology network of AIIMS were compromised by unknown threat actors due to improper network segmentation, which caused operational disruption due to non-functionality of critical applications. CERT-In and other stakeholder entities advised necessary remedial measures in respect of the same.

(c): As per the information reported to and tracked by CERT-In, the number of cyber security incidents during the years 2018, 2019, 2020, 2021 and 2022 are 2,08,456, 3,94,499, 11,58,208, 14,02,809 and 13,91,457 respectively.

(d) and (e): The National Security Council Secretariat (NSCS) has formulated a draft National Cyber Security Strategy, which aims at holistically addressing issues of security of the national cyberspace.

****