GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3492
TO BE ANSWERED ON: 22.03.2023

CYBER ATTACKS ON GOVERNMENT WEBSITES AND HEALTH INSTITUTIONS

3492. SHRI K. MURALEEDHARAN:
DR. AMAR SINGH:
ADV. ADOOR PRAKASH:
SHRI VINCENT H. PALA:

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

(a) the details of the total number of cyber attacks on Government websites and health institutions such as public and private hospitals and insurance agencies since 2014, year wise;
(b) whether the draft National Cyber Security Strategy will include measures for protection of Indian Cyber Security infrastructure to prevent large scale data breaches such as that of 3.8 crore DigiLocker accounts in 2020 or the 110 crore Aadhaar accounts in 2018;
(c) if so, the details thereof and if not, the reasons therefor; and
(d) the details of the measures proposed to be taken by the Government to protect Government websites in particular under the aforementioned strategy?

ANSWER

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

(a): Government is committed to ensure that Internet in India is Open, Safe and Trusted and Accountable for its users and is cognizant of various cybersecurity threats. With emergence of new technology and rise in the usage of Internet, increase in cyber incidents is a global phenomenon.

The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cybersecurity incidents in India. Information reported to and tracked by CERT-In, is as under:

Year	Government agencies, institutions and undertakings	Websites of Central Ministries/Departments and State Governments	Health institutions
2014	3,719	155	561
2015	4,916	164	887
2016	5,416	199	935
2017	33,514	172	1,030
2018	70,798	110	665
2019	85,797	54	1,108
2020	54,314	59	2,889
2021	48,285	42	1,904
2022	1,92,439	50	2,712

(b) and (c): Government has undertaken the finalisation of a National Cyber Security Strategy (NCSS) that holistically looks at all issues of security in the national cyberspace, capture all cyber-threat concerns, detail the mechanism and roadmap for the protection of

India’s digital assets, especially critical information infrastructure, and capacity building activities to deal with cyber-attacks.

(d): The measures proposed to be taken by the Government to protect government websites in particular, under the aforementioned strategy are as follows:

(i) Build and implement a comprehensive risk profile, assessment, management and maturity index framework for all critical functions and processes in critical sectors;
(ii) Create a reference framework for secure software and hardware development adopted by government and industry alike;
(iii) Establish a National Threat Exchange and build a National Cyber Risk Registry;
(iv) Create a National Bug Bounty Programme in close support and coordination with the industry; and
(v) Mandate various agencies to audit websites.

****