GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2644
TO BE ANSWERED ON: 11.08.2023

DATA BREACH OF SENSITIVE AND PERSONAL DATA

2644. SHRI MALLIKARJUN KHARGE:

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

(a) whether Government maintains a list of cyber security incidents leading to data breaches, data loss, etc, that have affected departments, Ministries or organisations under Government, specifically data breaches in cases of CoWin, AIIMS, EPFO and UIDAI;

(b) if so, the details of security incidents that have led to data theft or loss of data and action taken by Government in such cases; and

(c) if not, the reasons therefor?

ANSWER

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

(a) to (c): Yes Sir.

The Government is committed to ensure that the internet in India is safe, trusted and accountable for all users. With the expansion of the internet and more and more Indians coming online, instances of cyber incidents have also increased. Government is fully cognizant and aware of various cyber security threats. The Indian Computer Emergency Response Team (CERT-In) maintains a list of cyber security incidents leading to data breaches and data leaks.

As per the information reported to and tracked by CERT-In, a total number of 0, 0, 14, 6, 27 and 15 data leak incidents and total number of 5, 11, 36, 39, 51 and 49 data breach incidents are observed during the year 2018, 2019, 2020, 2021, 2022 and 2023 (upto June) respectively.

Data breach/theft incidents are normally caused by a combination of factors, including exploitation of vulnerable services, misconfigurations, compromised credentials, malware infections and third-party breaches.

Government has taken following measures to enhance the cyber security posture and prevent data breaches:

(i) On observing the data breaches and data leaks, CERT-In notifies the affected organisations along with remedial actions to be taken. CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as law enforcement agencies.

(ii) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.

(iii) A special advisory on security practices to enhance resilience of health sector entities has been communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitising health sector entities regarding latest cyber security threats in December 2022. The Ministry has been requested to disseminate the advisory among all authorised medical care entities / service providers in the country.

(iv) CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(v) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

(vi) CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

(vii) Government has formulated a Cyber 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.

****