GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3462
TO BE ANSWERED ON: 22.03.2023

CYBER ATTACKS INVOLVING EXAM LEAKS

3462. SHRI KESINENI SRINIVAS:

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

(a) the details of the number of cyber attacks responded to by CERT-IN explicitly pertaining to those which involve exam leaks;
(b) whether there have been any data breaches of the Central Government database during the last four years and if so, details thereof along with the loss of data due to such breach including the remedial measures taken by the Government in this regard; and
(c) the details of the number of cases registered and those solved, by CERT-IN since 2019,State/UT wise?

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 fully cognizant and aware of various cybersecurity threats. With emergence of new technology and rise in the usage of Internet, increase in cyber incidents is a global phenomenon.

As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), two incidents pertaining to examination leaks were reported and responded by the CERT-In, since 2019.

(b) and (c): As per information reported to and tracked by CERT-In, a total number of six data breach incidents pertaining to Central Government organisations were observed during the years 2019 to 2022 respectively.

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

(a) CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies, and notifies the affected organisations regarding cyber incidents, along with remedial actions to be taken.
(b) CERT-In issues alerts and advisories on an ongoing basis regarding the latest cyber threats/vulnerabilities and countermeasures to protect computers and networks.
(c) CERT-In has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats. It 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.
(d) CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism, for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.
(e) CERT-In regularly conducts training programmes for network and system administrators and chief information security officers of government and critical sector organisations, regarding securing the information technology infrastructure and

mitigating cyber-attacks. A total of 42 training programmes were conducted, covering 11,486 participants, during the years 2021 and 2022.

(f) Government websites and applications are audited with respect to cybersecurity and compliance with the Government of India Guidelines for Websites, prior to hosting.

(g) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(h) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cybersecurity tips and best practices for citizens and organisations.

(i) Cybersecurity mock drills are being conducted to enable assessment of cybersecurity posture and preparedness of organisations in the government and critical sectors. 74 such drills have so far been conducted by CERT-In, in which 990 organisations from various States and sectors participated.

(j) Security tips are published for users to secure desktops and mobile phones and to prevent phishing attacks.

(k) CERT-In regularly disseminates information and shares security tips on cybersafety and cybersecurity through social media handles and websites. It organised various events and activities for citizens during the Safe Internet Day on 8.2.2022 and the Cyber Security Awareness Month in October 2022, by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with the Centre of Development of Advanced Computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices, etc. through videos and quizzes on MyGov platform.

(l) CERT-In and the Reserve Bank of India jointly carry out a cybersecurity awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India platform.

(m) The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

****