GOVERNMENT OF INDIA

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

LOK SABHA

UNSTARRED QUESTION NO. 2868

TO BE ANSWERED ON: 17.12.2025

AI POWERED CYBER ATTACKS

2868. MR PATHAN YUSUF:

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

(a) the number of Artificial Intelligence (AI) powered cyber-attacks faced by the Indian firms during the last three years, year-wise;

(b) the average number of days within which Indian firms have reported cyber-attacks to the Government during the last three years, year-wise;

(c) whether the Government is aware of Indian firms paying ransom to regain access to their data;

(d) if so, the details thereof including the amount paid by Indian firms as ransom during the last three years, year-wise; and

(e) the number of cases in which Indian firms have been able to fully regain access to data after a cyber-attack during the last three years, year-wise?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY

(SHRI JITIN PRASADA)

(a) to (e): The policies of the Government are aimed at ensuring an Open, Safe and Trusted Internet for its users. In the rapidly evolving AI landscape, there is an increased risk of AI-enabled cyber-attacks and the government remains conscious of these.

The Indian Computer Emergency Response Team (CERT-In) has been designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology (IT) Act, 2000.

As per the information reported to and tracked by CERT-In, the total number of cyber security incidents related to Indian entities observed during the last three years are given below:

Year	Number
2022	11,99,018
2023	13,88,073
2024	7,31,988

Indian firms have reported cyber security incidents noticed by them to CERT-In within average of 2 days in 2022 and within 1 day during 2023 and 2024.

The Government has undertaken several measures to strengthen security of cyber ecosystem, inter alia, includes:

1. CERT-In advises organizations and individuals to refrain from making ransom payments in ransomware incidents.
2. Organizations implementing reasonable cyber security practices, particularly those securing backups are noticed to be able to restore data from unaffected backup sources.

3. CERT-In issues alerts & advisories regarding latest cyber threats/vulnerabilities including ransomware and countermeasures regularly.
4. It advises remedial measures to affected organisations and coordinates incident response measures.
5. CERT-In has also published “India Ransomware Report 2024” in March 2025, covering latest tactics and techniques of ransomware attackers and ransomware specific incident response and mitigation measures.

******