GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**RAJYA SABHA**
**UNSTARRED QUESTION NO. 1060**
TO BE ANSWERED ON: 10.02.2023

## INCREASING CASES OF CYBER-ATTACKS

**1060 # SHRI SANJAY SINGH:**

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

(a) the number of Indian companies operating in the country that had to face ransomware and such cyber attacks during 2014 to 2022, year-wise details thereof;
(b) the details of cyber attacks on Government agencies, institutions and undertakings during the said period;
(c) the details of data theft and economic loss due to cyber attack during the said period, year-wise; and
(d) the year-wise details of the plan implemented to prevent cyber attacks, cases registered and action taken during the said period?

## ANSWER

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

(a): Government is fully cognizant and aware of various cyber security threats and is committed to ensure that the Internet in India is Open, Safe and Trusted and Accountable for all its users. With innovation in technology and rise in usage in the cyberspace and digital infrastructure for businesses and services, cyber-attacks pose a threat to confidentiality, integrity and availability of data and services, which may have indirect or direct impact on the economy of businesses and service providers. Such economic impact is specific to the impacted entity, and depends on the extent to which its data, assets and services are affected by such attacks.

The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. As per the information reported to and tracked by CERT-In, a total of 0, 2, 21, 35, 26, 23, 41, 111 and 198 ransomware incidents and such cyber-attacks affecting Indian companies operating in the country were observed during the years 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 respectively.

(b): A total of 3,719, 4,916, 5,461, 33,514, 70,798, 85,797, 54,314, 48,285 and 1,92,439 cyber security incidents related to government agencies, institutions and undertakings were observed during the years 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 respectively.

(c) and (d): Data on crime is maintained by the National Crime Records Bureau. As per the National Crime Records Bureau, 9,622, 11,592, 12,317, 21,796, 27,248, 44,735, 50,035, 52,974 cases were registered under the category “cyber-crimes” during the year 2014, 2015, 2016, 2017, 2018, 2019, 2020 and 2021 respectively.

A number of measures have been taken to enhance India’s cyber security posture and to curb such incidents. These include the following:

(i) A Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism, has been formulated by CERT-In, for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.

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

(iii) Regular training programmes for network and system administrators and the Chief Information Security Officers of government and critical sector organisations are conducted by CERT-In, for securing the information technology infrastructure and mitigating cyber-attacks. A total number of 190 training programmes were conducted, covering over 16,000 participants since 2014.

(iv) CERT-In has been issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks, on an ongoing basis.

(v) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is operated by CERT-In to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

(vi) 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.

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

(viii) Cyber security mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the government and critical sectors.

(ix) The National Cyber Coordination Centre has been set up to generate situational awareness regarding existing and potential cyber security threats.

(x) CERT-In and the Reserve Bank of India (RBI) jointly carried out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

******