GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 559
TO BE ANSWERED ON: 07.02.2025

ASSESSMENT OF CYBERSECURITY RISKS DUE TO INCREASED DIGITISATION

559. DR. SYED NASEER HUSSAIN:

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

(a) whether Government has assessed cybersecurity risks associated with the rapid digitization of public services, and if so, the details thereof, and if not, the reasons therefor;
(b) the details of funds allocated/utilized for cybersecurity initiatives in the last five years;
(c) the steps taken to enhance cybersecurity preparedness, threat detection and incident response capabilities;
(d) the progress made in implementing and auditing security standards/frameworks for cloud service providers handling Government data; and
(e) the steps taken to promote indigenous cybersecurity solutions and reduce dependency on foreign security products?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a): The policies of the Government are aimed at ensuring an open, safe,trusted and accountable internet for its users. Government has taken several legal, technical, and administrative policy measures for addressing cyber security challenges in the country. The Government has issued directions to public service entities for regular audit to be conducted and reports to be submitted. Further, Indian Computer Emergency Response Team (CERT-In) has issued guidelines on Information security practices for Government entities in June 2023, covering domains such as security auditing, data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring and incident management. Cert-In has empanelled 191 security auditing organisation to support and audit implementation of Information Security Best Practices.

(b): The details of funds utilized for cybersecurity initiatives in the last five years are:

Non - Scheme - Establishment & Capital Budget Head (including Machinery & Equipment (M&E) later renamed as Information, Computer, Telecommunication (ICT) Equipment)

Amount in Crore

Year	Actual Expenditure
2019-20	29.9
2020-21	91.7
2021-22	193.7
2022-23	176.5
2023-24	249.2

Scheme - "Grant in Aid under " Cyber Security projects" including NCCC, R&D in Cyber Security Division, MeitY & Cyber Law and Data Governance Division, MeitY"

Amount in Crore

Year	Actual Expenditure
2019-20	92.0

2020-21	80.0
2021-22	322.1
2022-23	30.1
2023-24	316.5

(c): The Government has taken various measures to enhance cybersecurity preparedness, threat detection and incident response capabilities. These include:

i. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
ii. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.
iii. CERT-In regularly coordinates with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and devise appropriate proactive and preventive measures.
iv. CERT-In has issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024. SBOM helps organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.
v. CERT-In issued alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis. In this context, an advisory on safety measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications was published in May 2023.
vi. CERT-In has issued an advisory to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.
vii. CERT-In has released awareness posters on AI and IoT security through its social media handles to educate the users on the best practices that can be followed to stay protected against AI and IoT related threats.
viii. On observing data breach / data leak incidents, 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 as well as Law Enforcement Agencies.

(d): MeitY has empanelled both domestic and global Cloud Service Providers (CSPs) that guarantee data residency within India and adhere to Indian legal frameworks. These CSPs undergo rigorous audits by the Standardisation Testing and Quality Certification Directorate and comply with international security standards (ISO) such as ISO 27001, ISO 27017, ISO 27018, and ISO 20000. Additionally, CSPs go through periodic security audits to ensure that they meet the ever-evolving security guidelines and compliances mandated by the Government of India.

(e): Steps taken by the Government to promote indigenous cybersecurity solutions and reduce dependency on foreign security products inter-alia, include:

i. MeitY has funded various Research and Development projects in thrust areas of cyber security.

ii. MeitY has issued Public Procurement (preference to Make in India) Order 2019 for Cyber Security Products for promoting indigenous cybersecurity solutions in the country.

iii. MeitY has launched the Cyber Security Grand Challenge to provide impetus towards product innovation in the Cyber Security start-up ecosystem.

****