GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**RAJYA SABHA**
**UNSTARRED QUESTION NO. 2130**
TO BE ANSWERED ON: 09.08.2024

## MICROSOFT OUTAGE

**2130. SHRI RAJEEV SHUKLA:**

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

(a) whether Government has taken cognisance of the recent global outage of Microsoft's services that affected various sectors of the economy;
(b) if so, the details thereof;
(c) the details of measures being taken by Government to ensure resilience during such occurrence in future;
(d) the proposed measures to be taken thereof to ensure an overall resilient digital ecosystem?

## ANSWER

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

(a) to (d): The Global outage was observed on 19 July 2024 around 9.40 AM IST. Microsoft systems in various organisations showed error messages and stopped functioning. The stoppage of the systems was caused due to a software update provided on to a cyber threat detection solution provided by a cyber security partner company. This issue affected organisations and users globally including in India where services of airlines, manufacturing and IT sector were impacted for few hours.

Indian Computer Emergency Response Team (CERT-In) coordinated with M/s Microsoft and its cyber security partner company regarding the outage. Microsoft’s cyber security partner identified it as a content deployment related issue and rolled back the changes. CERT-In has published an advisory on its website on 19 July 2024, providing remedial measures to fix the issue.

There was no impact of the recent outage in the Microsoft services on the IT systems and applications of Reserve Bank of India (RBI). National Data Centres of National Informatics Centre (NIC) were not affected

The policies of the government are aimed at ensuring an open, safe, trusted and accountable internet for its users. Government has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

(i) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.
(ii) CERT-In works in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.
(iii) 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.
(iv) CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-

empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.

(v) CERT-In has empanelled 176 security auditing organisations to support and audit implementation of Information Security Best Practices.

(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) 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.

(viii) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) 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.

(ix) CERT-In 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.

(x) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 92 such drills have so far been conducted by CERT-In where around 1,400 organizations from different States and sectors participated.

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

(xii) CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

(xiii) CERT-In regularly conducts trainings / workshops to train technical staff of Government, Public and Private sector organizations including StartUps and Micro, Small and Medium Enterprises (MSMEs) across all sectors on focused topics of Cyber Security. During 2024, till June, CERT-In has conducted 9 trainings on various specialized topics of cyber security covering 4,166 participants including system/Network Administrators and Chief Information Security Officers (CISOs).

(xiv) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.

(xv) CERT-In regularly carries out various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds

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

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

*******