CYBER SECURITY INCIDENTS

2757.　　　**SHRI K SUDHAKARAN:**
　　　　　SHRI SUKHDEO BHAGAT:
　　　　　SHRI C M RAMESH:

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

(a)　whether the Government has any plan to develop cyber security software tie up with Windows Operating System and cloud services brought various services in sectors like aviation, banking, hospitals, broadcasting, etc., standstill on 19th July, 2024 global tech outage and if so, the details thereof;
(b)　whether it is a fact that nearly 500 flights in India cancelled/postponed due to above malfunctioning of system and resorted to with manual processes and if so, the details thereof along with other sectors impacted in the country;
(c)　whether the Government is aware of that it has security incident or cyber attack and Russia and China insulated from this major disruption; and
(d)　whether the Government is developing its own Windows and Operating System to insulate our sectors from such malfunctioning and cyber attacks and if so, the details thereof?

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. Windows computers in various organisations showed error messages and stopped functioning. The stoppage of Windows 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. None of National Informatics Centre (NIC) and other Government Systems were impacted by the outage.

Government has supported the development of following solutions which inter-alias include:

i.　Meghdoot Cloud suite is a comprehensive free and open-source cloud suite. It is carved from Open Stack along with other solutions and in house developments. This Cloud suite transforms the conventional data centre into a Cloud offering Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and provision to offer Software as a Service (SaaS) with ease of management and operations. The suite encompasses solutions on a plug and play architecture and it ensures customization to meet the business needs of clients. The suite has unified dashboard for cloud operations and automated deployment of the stack. It supports for multiple hypervisors and heterogeneous environments.

ii. Bharat Operating System Solutions (BOSS) Linux is developed by the Centre for Development of Advanced Computing. BOSS has an enhanced desktop environment that includes support for various Indian language and instructional software.

iii. C-DAC has evolved a hardened variant of Mobile Operating System supporting specific Commercial off-the-shelf software (COTS) devices. This Mobile Operating System provides an enforcement of custom security policies at platform and kernel layers.

In addition, in order to protect all users from cyber attacks and malware attacks. Government has taken the following steps:

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

(ii) 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.

(iii) CERT-In provides automated cyber threat intelligence for organisations across sectors in near real time for proactive threat mitigation actions by them.

(iv) 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.

(v) CERT-In has empanelled cyber security auditing organisations to ensure the Information and Communications Technology (ICT) systems deployed in organizations are hardened.

(vi) Cyber security mock drills and exercises are being conducted regularly by CERT-In to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors to deal with cyber crisis situations.

(vii) CERT-In co-operates, works and coordinates incident response measures with affected organisations, international CERTs, overseas organisations, service providers and Law Enforcement Agencies.

****