GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA
UNSTARRED QUESTION NO: 1038
ANSWERED ON THE MONDAY, 2 DECEMBER, 2024/11 AGRAHAYANA, 1946 (SAKA)

STATUS OF CYBERSECURITY FRAMEWORKS IN BANKING SECTOR/PSBs

1038. SHRI BENNY BEHANAN:
SHRI ANTO ANTONY:
SHRI TANUJ PUNIA:
SHRI K SUDHAKARAN:

Will the Minister of FINANCE be pleased to state:

(a) the current status of cybersecurity frameworks implemented in Public Sector Banks (PSBs);

(b) the list of PSBs compliant with the latest security protocols;

(c) the specific challenges encountered in safeguarding financial data against cyber threats, particularly in the context of increasing digital transactions and online banking services;

(d) the steps taken to address these challenges and enhance the resilience of financial institutions against cyber attacks; and

(e) the measures taken/being taken by the Government to monitor and evaluate the effectiveness of these cybersecurity measures?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(SHRI PANKAJ CHAUDHARY)

(a) & (b): Reserve Bank of India (RBI), from time to time, issues various circulars/ guidelines to the banks including the Public Sector Banks (PSBs) to strengthen their cyber security framework. These circulars/ guidelines are required to be implemented by the banks. These, inter-alia, include the followings:

- Comprehensive Cyber Security Framework in Banks dated June 2, 2016 which mandates the banks to put in place a board approved cyber security policy, Security Operation Center, Cyber Crisis Management Plan etc.
- Master Direction on Digital Payment Security Controls dated February 18, 2021 which mandates the banks for implementation of common minimum standards of security controls for various payment channels like internet, mobile banking, card payment etc.
- Master Direction on Outsourcing of Information Technology Services dated April 10, 2023 which provides a framework for managing risks related to outsourcing of Information Technology (IT) services, managing concentration risk, outsourcing within a group or conglomerate, and specific requirements on the usage of cloud computing services.

- Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices dated November 7, 2023 which emphasizes enhancing IT governance, risk management, and assurance practices within the banks.

(c) & (d): With the increasing digitization and penetration of digital transactions, the exposure of cyber threats to the banks has also increased over time. In order to strengthen the cyber security posture of the banks, RBI has issued various guidelines/ advisories to plug the potential vulnerabilities and prevent frauds, data theft and other malicious activities. Further, Indian Computer Emergency Response Team (CERT-In) issues alerts & advisories on the latest cyber threats and suggests countermeasures on regular basis to ensure safe usage of digital technologies. Besides, banks also conduct periodic IT and System audits by auditors empanelled by CERT-In.

(e): As per the regulatory framework, banks are mandated to report all unusual cyber incidents to RBI within two to six hours of occurrence of such incidents. The implementation of cyber security related guidelines is assessed periodically through onsite and offsite inspections by the Cyber Security & IT Examination (CSITE) team of RBI. Banks are mandated to address the vulnerabilities noted, if any, during such inspections. Further, enforcement actions are initiated against the banks for non-compliance of such directions issued by RBI.

******