GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2504
TO BE ANSWERED ON: 15.03.2023

NEW NATIONAL CYBER SECURITY POLICY

2504. SHRI VIJAYAKUMAR (ALIAS) VIJAY VASANTH:

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

(a) whether the Government has introduced a new National Cyber Security Policy in the light of recent cyber attacks on bank/financial institute websites;
(b) if so, the details thereof along with the proposed timelines for its implementation and if not, the reasons therefor;
(c) whether the Government is aware that the lack of adequate cyber security and the dearth of talent in banking could potentially lead to a further rise in cyber attacks on user devices;
(d) whether the Government has taken any steps to mitigate citizens' vulnerability to cyber attacks;
(e) if so, the details thereof and if not, the reasons therefor; and
(f) whether the Government intends to coordinate with other countries to develop a global legal framework on cyber terrorism and if so, the details thereof?

ANSWER

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

(a) and (b): The Government is committed to ensure that the Internet in India is Open, Safe and Trusted and Accountable for its users. Keeping this in view, Government published National Cyber Security Policy 2013 to build a secure and resilient cyberspace for citizens, businesses and Government, and the mission of protecting information and information infrastructure in cyberspace, building capabilities to prevent and respond to cyber threats, reducing vulnerabilities and minimising damage from cyber incidents, through a combination of institutional structures, people, processes, technology and cooperation. Further, the Ministry of Home Affairs has issued National Information Security Policy and Guidelines to the Central Ministries as well as State Governments and Union territories with the aim of preventing information security breaches and cyber intrusions in the information and communication technology infrastructure. In addition, the National Security Council Secretariat (NSCS) has formulated a draft National Cyber Security Strategy 2021, which holistically looks at addressing the issues of security of national cyberspace.

(c) to (e): With the innovation of technology and rise in usage of cyber space and digital infrastructure for businesses and services, rise in cyber-attacks is a global phenomenon. Measures are taken to prevent cyber-attacks by deploying appropriate security controls and capacity building in organisations and enhancing awareness among users for safe usage of digital technologies.

Government and the institutions concerned with cybersecurity, including the Indian Computer Emergency Response Team (CERT-In) and the Reserve Bank of India (RBI), are fully cognizant and aware of various cybersecurity threats and has taken following measures to mitigate citizens vulnerability to cyber-attacks:

(i) RBI has issued various instructions in respect of security and risk mitigation measures related to electronic/digital transactions. These cover securing card transactions, securing payments through Internet banking / electronic payments, ATM transactions, prepaid payment instruments (PPIs), limiting customer liability on unauthorized electronic banking transactions, including PPIs issued by authorised non-banks, safeguarding against email spoofing attacks, etc.

(ii) As per the "Guidelines on Information Security, Electronic Banking,Technology Risk Management and Cyber Frauds" issued by RBI, banks need to have IT-related strategy and policies that cover, among other things, the desired number and level of information technology expertise or competencies in the bank's human resources, the plan to bridge the gap, if any, and the requirements relating to their training and development.

(iii) On observing a 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.

(iv) CERT-In operates the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats.

(v) 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.

(vi) 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.

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

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

(ix) The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs has been designated as the nodal point in the fight against cybercrime. A toll-free number 1930 has been made operational for citizens to get assistance in lodging online complaints in their own language. To spread awareness on cybercrime, the Ministry of Home Affairs has taken several steps that include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

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

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

(xii) 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.

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

(f): Pursuant to United Nations General Assembly resolution 75/282, adopted in May 2021, an Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes was established with all member states of the United Nations as part of the Ad Hoc Committee. India has proposed criminalisation of cyber terrorism under the Convention.

****