Government of India
Ministry of Finance
Department of Economic Affairs

LOK SABHA
UNSTARRED QUESTION NO. 2036
TO BE ANSWERED ON FRIDAY, DECEMBER 29, 2017/PAUSHA 08, 1939 (SAKA)

PROTECT SECURITY MARKETS FROM CYBER ATTACKS

QUESTION

2036. SHRI P.C. MOHAN

Will the Minister of FINANCE be pleased to state:

(a) whether the Securities and Exchange Board of India (SEBI) proposes to protect and safeguard the interests of the security markets from cyber attack/threats;

(b) if so, the details thereof and if not, the reasons therefor;

(c) whether the Government has received any report from the security markets or from SEBI regarding any cyber attack on their database; and

(d) if so, the details of such cyber attacks during the past three years and the current year?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF FINANCE
(SHRI PON RADHAKRISHNAN)

(a) and (b): Securities and Exchange Board of India (SEBI), the securities markets regulator, has informed that it has introduced Cyber Security and Cyber Resilience framework for Registrars to an Issue / Share Transfer Agents (RTAs) vide SEBI's circular dated September 8, 2017, wherein the Qualified RTAs servicing for more than 2 crore folios are required to adhere to the framework as prescribed in the circular.

Further, SEBI and Stock Exchanges/Depositories have been issuing periodic advisories, various alerts and notices to the Market Infrastructure Institutions (MIIs) & respective intermediaries respectively, on various areas related to cyber security, including CERT-In (*The Indian Computer Emergency Response Team*) advisories, for information and necessary action for safeguard. It is also informed that SEBI is in consultation with Stock Exchanges/Depositories for framing bare minimum standards for cyber security and cyber resilience for all intermediaries.

It may also be noted that SEBI, vide its circular dated July 06, 2015, has laid down a detailed framework with regard to cyber security and cyber resilience that MIIs are required to adopt. The framework, inter-alia, covers areas such as governance, identification of critical assets and cyber risks (threats and vulnerabilities), access controls, physical security, network security management, security of data, hardening of hardware and software, application security and testing, patch management, disposal of systems and storage devices, vulnerability assessment and penetration testing (VAPT), monitoring and detection, response and recovery, sharing of information, training, and periodic audit.

SEBI has further informed that it has constituted a High Powered Steering Committee on Cyber Security (HPSC-CS), comprising experts such as Director General of CERT-In and member of SEBI's Technical Advisory Committee, to advise SEBI on various cyber security related areas for developing and maintaining cyber security and cyber resilience requirements aligned with best global practices, measures to improve cyber resilience and related business continuity and disaster recovery process in Indian securities market, etc.

(c) & (d): One incident of website defacement was reported from a security market firm in 2016 to the Indian Computer Emergency Response Team (CERT-In). CERT-In recommended the security best practices to strengthen the infrastructure so as to prevent occurrence of such incidents in future.

*****