GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 732
TO BE ANSWERED ON: 21.07.2017

INCIDENTS OF CYBER ATTACKS

732 SHRI ANIL DESAI:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether recently country faced a wave of cyber security incidents ranging from targeted attacks on Government organisations to ATM malware attacks, if so, the details thereof;
(b) whether the country is ill-prepared to combat potential risks associated with cashless transactions and pushing hundreds of millions of citizens' private information into the digital space; and
(c) if so, the steps Government is taking to deal with sophisticated financially motivated espionage actor groups focusing on critical systems and maturing business in 2017?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a): With the proliferation of Information Technology and related services, there is a rise in number of cyber security incidents in the country like elsewhere in the world. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455, 50362 and 27482 cyber security incidents were observed during the year 2014, 2015, 2016 and 2017 (till June) respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, targeted attacks, ATM malware, ransomware, Denial of Service attacks, etc.

(b) : No, Sir.

(c): Government is aware of the nature of the threats in Cyber Space. Accordingly, Government is following an integrated approach with a series of legal, technical and administrative steps to ensure that necessary systems are in place to enhance security of digital payment systems. In order to enhance safety of the digital technology and to prevent cyber attacks on critical financial systems, the following key actions have been taken, namely:-

i) All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised by Indian Computer Emergency Response Team (CERT-In) through the Reserve Bank of India to carry out audit by empanelled auditors of CERT-In on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

ii) All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

iii) Government has formulated Cyber Crisis Management Plan for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

iv) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. Till date, 15 such drills have been conducted by the CERT-In involving 148 organisations from different sectors including Finance sector.

v) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and mobile phones on regular basis. 25 advisories have also been issued regarding safeguards for users and institutions to secure digital payments.

vi) Government has established Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.

vii) Government has issued general guidelines for Chief Information Security Officers (CISOs) for securing applications and infrastructure and their key roles and responsibilities for compliance.

viii) CERT-In is regularly conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations to give an exposure on current threat landscape and countermeasures. In addition, CERT-In has also conducted a workshop on security of digital payments systems for stakeholder organisations covering 110 participants.

ix) Reserve Bank of India (RBI) has set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents.

x) Department of Banking Supervision under RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In.

xi) RBI has issued circular on 9th December 2016 on security and risk mitigation measure for all authorised entities / banks issuing Prepaid Payment Instrument (PPI) in the country.

xii) RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks.

xiii) RBI has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security.

xiv) RBI has set up a Cyber Security and IT Examination (CSITE) cell within its Department of Banking Supervision in 2015.

****