LOK SABHA SECRETARIAT
RESEARCH AND INFORMATION DIVISION

INFORMATION BULLETIN

No. LARRDIS (E&F) 2017/IB-2 AUGUST 2017

CYBER SECURITY IN THE FINANCIAL SECTOR

Introduction

Digital modes of transaction and communication are becoming increasingly important for strengthening the financial sector, thereby empowering the society and the economy. Acknowledging the benefits of digital operations, governments the world over are promoting digitization in the day-to-day functioning of their financial institutions. However, with the phenomenal increase in electronic transactions and rapidly growing digital economy, cyber attacks have become a matter of grave concern. Digitization, therefore, has not only brought opportunities; but has also exposed the economies to risks capable of creating major disruptions in the operations of the banking and other financial institutions.

A digitally-dependent set up with high connectivity brings with it the persistent threat of cyber attacks which has today become a matter of serious concern, particularly for the financial sector. The use of Information Technology (IT) for providing financial services has grown rapidly and is now an integral part of the operational strategy of all the banks and financial institutions. Alongside the increased use of internet banking and cutting edge technology-linked financial services, cyber risks have grown and cyber crimes have become increasingly sophisticated. Attackers now include "hacktivists", cyber criminals and terrorists who are motivated by financial gains to cause political and financial instability and collapse of the financial infrastructure.

Cyber security, or the defence of cyber space, is inherently an issue of international concern even from the perspective of national interest. Unlike national boundaries, cyber space is not well defined. It has no geographical or institutional limits. It is an independent environment consisting of interactions between people and software services enabling world-wide distribution of information and communication. Increasing Internet penetration is leading to an expansion of cyber space as its size is proportional to the activities that are carried through it. In such a scenario, technology adoption needs to be done causciously so that the possibilities of cyber risks are minimized.

Box-1
What is a Digital Economy

The term 'Digital Economy', coined by Don Tapscott, author of the 1995 best-selling book "The Digital Economy: Promise and Peril in the Age of Networked Intelligence", is the worldwide network of economic activities enabled by Information and Communications Technologies (ICT). It can also be defined more simply as an economy based on digital technologies.

The digital economy is not simply about moving business transactions from face to face to online; it is about transforming the ways business interactions and transactions are effected and also enabling economic-innovations. There are several key components of the digital economy. These are technology infrastructure consisting of the hardware, software and networks, the digital processes through which the business activities take shape and also the digital transactions through which customers buy and obtain products and services from the organizations.

The digital economy is continually evolving. Fueled by the growing use of personal computing devices, enterprise computing capabilities and Internet access, it is now being driven by more advanced digital technologies, notably wireless networks, mobile devices, positioning technologies (*i.e.*, GPS), embedded sensors and real-time analytics.

Cyber crime or cyber attack may also include computer network attack which is an attack by one computer to another *via* Internet. These crimes include stealing intellectual property of the individual/ organization and the nation, confiscation of online bank accounts and even disrupting critical infrastructure of a country. Only recently, the ransomware attack is estimated to have locked up more than one lakh computers across more than a hundred countries which highlights the real peril of cyber threats in the virtual world. Today, the frequency and impact of cyber-attacks have increased manifold and more so in the financial sector, underlining the urgent need to ensure adequate cyber security preparedness by the banks and financial institutions on a continuous basis. The issue has attracted attention globally, thereby making it to the top on the agenda of the governments across the world as also of the management of almost every organisation in the financial sector.

Fundamental Elements of Cyber Security for the Financial Sector

In view of the cyber risk growing more dangerous and threatening global financial systems, an expert group of G7 countries[1] prepared a report in 2016 on cyber security in the financial sector containing the fundamental elements that are intended to assist a financial sector entity to design and implement its cyber security strategy and operating framework as well as to guide public authorities in developing their policies. These elements are as following:

(i) **Cyber Security Strategy and Framework:** The purpose of a cyber security strategy and framework is to specify how to identify, manage and reduce cyber risks effectively in an integrated and comprehensive manner. Entities in the financial sector should establish cyber security strategies and frameworks tailored to their nature, size, complexity, risk profile and culture. Informed by the cyber threat and vulnerability landscape, a jurisdiction can also formulate sector-wide cyber security strategies and frameworks that outline how cooperation occurs between entities and public authorities in the financial sector, with sectors upon which the financial sector depends, and with other relevant jurisdictions.

(ii) **Governance:** Effective governance structures reinforce accountability by articulating clear responsibilities and lines of reporting. Effective governance also mediates competing objectives and fosters communication among operating units, information technology, risk and control-related activities. Consistent with their missions and strategies, boards of directors (or similar oversight bodies for public entities or authorities) should establish the cyber risk tolerance for their entities and oversee the design, implementation and effectiveness of the related cyber security programmes.

(iii) **Risk and Control Assessment:** Ideally, as part of an enterprise risk management programme, entities should evaluate the inherent cyber risk presented from any quarters. Entities should then identify and assess the existence and effectiveness of the controls to protect against the identified risks to arrive at the residual cyber risk. Protection mechanisms can include avoiding or eliminating risk by not engaging in an identified activity. They can also include mitigating the risk through controls or sharing or transferring the risk. Public authorities should map critical economic functions in their financial systems as part of their risk and control assessments to identify single points of failure and concentration risk.

(iv) **Monitoring:** Effective monitoring helps entities adhere to established risk tolerances and timely overcome weaknesses in the existing control system. Depending on the nature of an entity and its cyber risk profile and control environment, the testing and auditing functions should be appropriately aligned with the managing of the cyber-security programme.

(v) **Response:** As part of their risk and control assessments, entities should implement incident responsive policies and other control system to facilitate effective incident response. Among other things, these control systems should clearly address decision-making responsibilities within the entities.

(vi) **Recovery:** Once operational stability and integrity are assured, prompt and effective recovery of operations should be based on prioritization of critical economic and other functions and in accordance with objectives set by the relevant public authorities. Maintaining trust and confidence in the financial sector significantly improves when entities and public authorities have the ability to mutually assist each other in the resumption and recovery of critical functions, processes and activities. Therefore, before an incident occurs, establishing and testing contingency plans for essential activities and key processes, such as funding, can contribute to a faster and more effective recovery.

(vii) **Information Sharing:** Sharing technical information, such as threat indicators or details on how vulnerabilities were exploited, allows entities to remain up-to-date in their defences and learn about emerging methods used by attackers. Sharing broader insights among entities and public authorities deepens collective understanding of how attackers may exploit sector-wide vulnerabilities that could potentially disrupt critical economic functions and endanger financial stability. Given its importance, entities and public authorities should identify and address impediments to information sharing.

[1]Group of seven countries (G7) consisting of Canada, France, Germany, Japan, Italy, the United Kingdom and the United States.

(viii) **Continuous Learning:** Cyber threats and vulnerabilities evolve rapidly, as do the best practices and technical standards to address them. The composition of the financial sector also changes over time, as new types of entities, products and services emerge. Entity-specific as well as sector-wide cyber security strategies and frameworks need periodic review and update to adapt to changes in the threat and control environment, to enhance user awareness and to effectively deploy resources. Other sectors, such as energy and telecommunications, present external dependencies and, therefore, the entities and public authorities should consider developments in these sectors as part of any review process.

Digital India and Cyber Security

Digital India is a flagship programme of the Government of India with a vision to transform the country into a digitally empowered society and knowledge economy. As part of promoting cashless transactions and converting India into less-cash society, various modes of digital payments are available, which include e-wallet, Cards (Pre-paid, Debit, Credit), Point of Sale (PoS), Unified Payments Interface (UPI), Unstructured Supplementary Service Data (USSD) channel, etc.

However, the exponential growth in digital payments in India and a push towards less cash economy has renewed focus on the need to strengthen the country's financial cyber security infrastructure and preparedness. Banks and financial institutions are extremely vulnerable to various forms of cyber attacks and online frauds. In addition to core banking, services like e-banking, ATM and retail banking are increasingly becoming vulnerable to cyber crime. In 2015 alone, the Indian Computer Emergency Response Team (CERT-In)[2] reported over forty nine thousand cyber incidents, which included, among others, web intrusion, malware propagation, phishing, distributed denial of services attacks and web defacement. However, this number does not indicate the actual threat level, as companies and individuals are often negligent about security and reluctant to report cyber attacks. Individually, such attacks can't cause massive damage to the banking system but a co-ordinated approach with multiple attack tactics, which involve breaching and infecting systems with malware for information theft and similar other goals, pose a real threat.

In the financial year 2016-17, India witnessed serious cyber breaches. In one such instance, the hackers had penetrated the network of Hitachi, to which some banks had outsourced the processing of their ATM transactions. The holders of approximately 32,00,000 debit cards of these banks feared that their account details had been compromised as a result of the same. On performing forensic audit through a payments security firm which Hitachi had employed, it was found that the hackers had created a 'dummy code book' within the Hitachi system capturing all possible 4-digit numbers from 0000 to 9999 in an attempt to steal the Personal Identification Numbers (PIN) of the customers whenever they used their ATM cards. In another incident, USD 171 million was debited from the account of the Union Bank of India without authorization in a cyber-hacking operation. There were also cases of ransomware attack reported by various banks in India during the first two months of 2017.

Box-2
World-wide Cyber Attacks in the Recent Past

- **Phillippines:** The exclusion of casinos from the Anti-Money Laundering Act in Phillippines gave hackers a loophole to route money without coming into any scrutiny. Hackers issued instructions *via* SWIFT (Society for Worldwide Interbank Financial Telecommunication) network to steal up to USD 951,000,000 from the Bangladesh Central Bank's account with the Federal Reserve Bank of New York between 4th and 5th February 2016, when Bangladesh Bank's offices were closed. They were successful in stealing USD 101,000,000. Out of these, USD 81,000,000 were found in the Philippines (in five separate accounts with the Rizal Commercial Banking Corporation) and the remaining USD 20,000,000 in Sri Lanka (Shalika Foundation, a Sri Lanka-based company).
- **United Kingdom:** In January 2016, HSBC United Kingdom's website was hacked by hackers. Following this, internet banking was blocked for several hours. However, this incident did not result in loss of customer data.
- **Greece:** Activist hacker group "Anonymous" in January 2016, took the Bank of Greece offline for several minutes. However, the bank's defences quickly responded to it and there was no compromise of data.
- **Qatar:** In April 2016, Qatar National Bank was attacked by an unidentified cyber attack which resulted in loss of customer's data to a tune of up to 1.4 GB. The leaked data included files relating to staff at Al Jazeera, members of Qatar's ruling al-Thani family, and intelligence and defence officials.
- **Vietnam:** In May 2016, hackers attempted to steal USD 1,100,000 million from Vietnam's Tien Phong Bank. The attack involved use of instructions *via* SWIFT network. However, the bank's cyber defences responded quickly and no loss was caused.
- In May 2017, ransomware hit systems in over more than 100 countries including Russia and the United Kingdom infecting computers running an older version of XP, locking access to files.

[2]Indian Computer Emergency Response Team (CERT-In) is an organisation under the Ministry of Electronics and Information Technology. Under Section 70B of the Information Technology (Amendment) Act, 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security: (i) collection, analysis and dissemination of information on cyber incidents; (ii) forecast and alerts of cyber security incidents; (iii) emergency measures for handling cyber security incidents; (iv) coordination of cyber incident response activities; and (v) issue of guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

Types of Cyber Threats in the Banking and Financial Sector in India

From among the varied categories of banking and financial sector incidents reported to the Indian Computer Emergency Response Team (CERT-In), the threat actors have been increasingly observed to exploit the vulnerabilities and complexities in alternate channels such as ATMs, Point of Sale terminals and electronic wallets than the traditional phishing attacks, Distributed Denial of Service (DDoS) attacks, web defacement, etc. Broadly, the following types of cyber threats are there in India:

Attacks on ATMs

(a) **ATM Jackpotting/Spitting Malware Attacks:** Malware Green Dispenser facilitates localised hacking of a series of ATMs that operate on outdated software by providing the attacker the ability to walk up to the ATM and drain its cash vault without involving any wider network infections. The hack is 'physical' malware attack that involves plugging a device — say a laptop, phone or pendrive — into the dispenser's USB port to transfer an infected file or virus that causes the machine to behave erratically. When installed, Green Dispenser may display an "out of service" message on the ATM but the machine can be remotely controlled by a virtual keyboard and instructed to spew out cash. The malware then erases the tracks to avoid forensic detection.

(b) **ATM Skimming and Point of Sale (POS) Crimes:** It involves compromising the ATM machine or POS systems by installing a skimming device atop the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine. Additionally, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and Personal Identification Number (PIN) codes that are later replicated to carry out fraudulent transactions.

Phishing Scams

Phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords, usernames, login IDs, ATM PINs and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The phishing attackers direct the recipient to a web page (mirror webpage) exactly designed to look as a impersonated organization's (often bank & financial institution) own website and then they cleverly harvest the user's personal information, often leaving the victim unaware of the attack. It is usually carried out using free or paid phishing kits that comprise scripts, images, web server code and web pages. The paid kits allow their sellers to receive the files of stolen data from the backdoor. It can also manipulate the server where it is hosted. The scammers use social media websites, spam e-mails, Instant Messaging Services, blogs and text messages for the distribution of the links to the phishing websites.

Fraudulent Financial Transactions at International POS Terminals outside India

There have been instances when the fraudsters have successfully conducted transactions using the Indian Banks customers' stolen cards, track 2 data containing card holder's name, account number and other discretionary data which do not require PIN-based authentication.

Mobile Banking Exploitation

As many mobile banking apps have enabled customers to conduct financial transactions remotely using a mobile device such as a mobile phone or tablet, the application bugs have been increasingly targeted for stealing personal identifiable information and conducting fraudulent financial transactions also.

Targeted Disruption of Access to Bank Networked Systems and Services

(a) **Using Distributed Denial of Service (DDoS) by Bitcoin[3] extortionist cybercriminal gangs:** The threat actors use botnets[4] to direct large volumes of useless traffic to a target network with the intention of overpowering it. The attacks are preceded by emails from gang-members that have attempted to extort money from the targets, sharing details on how and where the victims would pay, and included a promise not to target them again if they complied with. Hackers use devices such as Close Circuit Television Cameras (CCTV) and mobile phones to carry out their activities.

(b) **Using Ransomware Trojans for Cyber Extortion:** Here the hackers seize control of computers at the banks using the ransomware to encrypt all files and demanding a ransom in bitcoins for the decryption keys to unfreeze them.

Advanced Persistent Threat (APT) Attacks

It is the targeting of bank systems directly to modify, delete and/or steal data. It is characterised as a set of complex, stealthy and ongoing computer hacking processes, often targeting a specific entity to intrude into a network by avoiding detection to siphon off

[3]Bitcoin is a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

[4]Botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, *e.g.* to send spam.

sensitive targeted information over a significant period of time. Typically, an APT involves a sequence of phases:

- Conducting extensive research to select an organisation that use IT systems that are exploitable.
- Footprinting to create a blueprint of the target's IT infrastructure to study details about its sites, network topology, domain, internal Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers, internal Internet Protocol (IP) address ranges and any other exploitable ports or services as captured.
- Malware engineering where the attackers plan the attack after they have identified their target's IT systems and exploitable vulnerabilities. They engineer or procure the core and supplementary malware required to carry out the attack.
- Initial breakthrough when the attackers phishes their target company's employees into downloading the malware or use some type of social engineering to gain access to the targeted network through legitimate means. Alternatively, they can also exploit any zero-day vulnerabilities of the software used by the employees.
- Capturing administrative privileges which in almost all of the attacks, the hackers attempt to steal the local administrator credentials of the victim's computer and subsequently steal domain-level administrative credentials.
- Privileged credential theft and backdoor establishment for siphoning of stolen data and to implant more malware for compromising more systems.
- Covering tracks to erase digital evidences of hack, intrusion, compromise and theft.

Insider Cyber Crimes

Insider Cyber Crimes are done by abusing access rights over different organisational network resources, theft of materials and mishandling physical devices. Several incidents occur in Banks due to Insider threats that include sabotage, theft, espionage, fraud and competitive advantage.

Initiatives Taken by the Government of India to Address Cyber Security Problem

The Government of India has taken several steps towards enabling secure online payment systems. The Reserve Bank of India (RBI) has also issued a list of do's and don'ts to the banks post-2016 incidence of cyber breach. However, at the same time it is widely acknowledged that the primary responsibility to avoid any mishap and for ensuring a fool-proof cyber security lies on the agencies involved in facilitating online transactions.

National Cyber Security Policy 2013

The main features of the National Cyber Security Policy 2013 are as follows:

- With an aim to monitor and protect information and strengthen defences from cyber attacks, the National Cyber Security Policy 2013 was released on 2 July 2013 by the Government of India. The purpose of this framework document is to ensure a secure and resilient cyberspace for citizens, businesses and the government.
- The Cyber Security Policy aims at protecting the information infrastructure in cyberspace, reducing vulnerabilities, building capabilities to prevent and respond to cyber threats and minimizing damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation.
- The objective of this policy in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A national and sectoral 24X7 mechanism has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC).
- Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for the coordination of crisis management efforts. CERT-In will also act as umbrella organization for coordination and operationalization of sectoral CERTs.
- A mechanism is proposed to be evolved for obtaining strategic information regarding threats to Information and Communication Technology (ICT) infrastructure, creating scenarios of response, resolution and crisis management through effective predictive, preventive, responsive and recovery action.
- The policy calls for effective public-private partnership and collaborative engagements through technical and operational cooperation.
- The policy also calls for developing human resource through education and training programmes, for establishing cyber security training infrastructure through public-private partnership and also for establishing institutional mechanisms for capacity-building for law enforcement agencies.
- Organizations are required to develop their information security policies properly dovetailed into their business plans and implement such polices as per international best practices.
- The policy document aims at encouraging all organizations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives.

- The policy also emphasises the promotion of research and development in cyber security.

The following major initiatives have been recently taken by the Government to address security concerns towards digital payments:

- Digital Payments Security Committee has been setup under the chairmanship of Secretary, Ministry of Electronics and Information Technology and co-chairmanship of the Secretary, Department of Telecommunications first meeting of this Committee was held on 31 March 2017.
- Ministry of Electronics and Information Technology has formulated draft Rules on Security of Prepaid Payment Instruments under the Information Technology Act, 2000[5]. The draft Rules have provision for grievance redressal mechanism for electronic prepaid payment instruments. The draft Rules have been published on Ministry of Electronics and Information Technology website inviting comments from the public at large and all stakeholders.
- Digital Payment Division has been setup at Ministry to tackle the challenges and improve the cyber security posture of the digital payment ecosystem.

Institutional Framework for Cyber Security in India

Indian Computer Emergency Response Team (CERT-In)

Indian Computer Emergency Response Team (CERT-In) is a functional organization under the Ministry of Electronics and Information Technology with the objective of securing Indian cyber space. CERT-In provides incident prevention and response services as well as security quality management services. CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. The organisation has taken the following initiatives:

- CERT-In has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism for implementation by all Ministries/Departments of the Central Government, State Governments and their organizations and other critical sectors. CERT-In regularly interacts with the Reserve Bank of India (RBI), Institute for Development and Research in Banking Technology (IDRBT) and Banks to enable implementation of CCMP.
- Cyber security exercises are confidence-building and learning exercises based on simulated and hypothetical cyber security incident scenarios. Exercises are intended to be collaborative and coordinated in the interface between CERT-In and organizations in key sectors. Cyber security exercises are being conducted regularly by CERT-In for assessment of cyber security posture and preparedness of the organizations in the Government and critical sectors. Two finance sector-specific cyber security exercises were conducted by CERT-In in 2016.
- CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out.
- Cyber *Swachhta Kendra* (Botnet Cleaning and Malware Analysis Centre) was established by CERT-In in February 2017 for detection of compromised systems in India and also for the prevention of further malware infections. The centre is working in close coordination and collaboration with the Internet service providers, academia and industry. The centre is providing detection of malicious programmes and free tools to remove the same for common users. The centre is also working with Banks to detect malware infections in their networks and enable remedial actions.
- CERT-In regularly sends advisory to the Reserve Bank of India, National Payment Corporation of India (NPCI) and Payment Card Industry organisations regar2ding the threats targeting banking and ATM systems. The advisory covers best practices to strengthen the security of ICT systems. For the financial sector, CERT-In has issued 23 advisories for security safeguards covering Point of Sale (POS), Micro ATMs, electronic Wallets, online banking, smart phones, unified payment interface, Unstructured Supplementary Service Data (USSD), RuPay, SIM cards, wireless access points/routers, mobile banking, cloud and *Aadhaar* Enabled Payment System (AEPS).
- CERT-In conducts regular training programme to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber attacks. 18 such training programmes were conducted covering 580 participants during the year 2016.
- CERT-In is contributing as a member of Inter-disciplinary Standing Committee on Cyber Security to review the threats inherent in the existing/emerging technology; by study adoption of various security standards/ protocols; interface with stakeholders; and to suggest appropriate policy interventions to strengthen cyber security and resilience in financial sector.

[5]An Act of the Parliament which aims at providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. The Act was further amended as the Information Technology (Amendment) Act, 2008.

- Regular workshops with IDRBT for banks, RBI, Securities and Exchange Board of India (SEBI) are conducted on cyber security. CERT-In officials are deputed as trainer at IDRBT.

Financial Computer Emergency Response Team (CERT-Fin)

The budget announcement of 2017 by the Finance Minister of India regarding the setting up of a Computer Emergency Response team in the Financial Sector (CERT-Fin) reflects the importance the Government of India is attaching to cyber security in the financial sector. The rationale behind this proposed CERT-Fin plan is to set up an integrated cyber security framework connecting country's top finance regulators, institutions and stakeholders with security response unit. This will lead to a better co-ordination, control and response to any incident and event linked to cyber crimes and threats that could impact India's financial sector.

Once CERT-Fin is in place, this will bring sophisticated digital security, assets capability and controls, making India an exemplary global leader in data security and privacy. It will create general security awareness across the country and play a key role in bringing together Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) in the financial sector and security specialists in India, thereby promoting a collaborative platform for bringing in place an effective cyber security framework. And more than anything else, CERT-Fin will facilitate implementation of stronger data-protection policies and security framework along with mandatory security practices or policies that financial institutions need to comply with.

Initiatives taken by the Regulators

(i) Reserve Bank of India (RBI)

Recognising the growth in the cyber attacks on banks in India, the RBI has taken several key initiatives and critically important steps to strengthen cyber security preparedness in the banks. RBI has issued a comprehensive circular on Cyber Security Framework in Banks on 2 June 2016 covering best practices pertaining to various aspects of cyber security. Some key features of the Cyber Security Framework are as under:

- Banks to classify risks in four categories, namely low, moderate, high and very high, and mandatorily report any unusual behavior in their servers/networks to RBI.
- Banks to set up a Security Operations Centre (SOC) for performing continuous surveillance and remain updated about cyber threats.
- The IT architecture, which shall facilitate smooth functioning of such policy, should be reviewed continuously.
- Banks to evolve a Cyber Crisis Management Plan (CCMP). The CCMP should address four aspects namely, (i) detection; (ii) response; (iii) recovery; and (iv) containment. To audit the adequacy of cyber resilience framework, certain indicators shall be developed and tested by independent qualified professionals. In addition, banks have also been directed to create awareness about cyber security amongst all the stakeholders.
- Certain minimum cyber security and resilience requirements and guidelines for setting up and operating of the SOC have been specified.

This apart, the RBI periodically conducts cyber drills in co-ordination with CERT-In. As announced in the Bank's sixth bi-monthly Monetary Policy Statement for 2016-17, an inter-disciplinary Standing Committee on Cyber Security has been constituted to review the threats inherent in the existing/emerging technology; to study adoption of various security standards/protocols; to interfere with stakeholders; and to suggest appropriate policy interventions to strengthen cyber security and resilience. The Committee has been meeting regularly and as per its recommendations, sub-groups are formed on certain focus areas for in-depth examination. The RBI has also established an IT Subsidiary named Reserve Bank Information Technology Pvt. Ltd. which focuses *inter alia* on cyber security within RBI as well as in regulated entities. The RBI has also performed comprehensive IT examination of the major banks to assess their cyber risk resilience and response. Remedial action by the banks are also closely monitored by the RBI.

(ii) Securities and Exchange Board of India (SEBI):

A High Powered Steering Committee on Cyber Security (HPSC-CS) has been setup by SEBI. The broad terms of the Committee include:

- to oversee and provide overall guidance on cyber security initiatives for SEBI and for the entire capital market;
- to advise SEBI in developing and maintaining cyber security and cyber resilience requirements aligned with global best practices and industry standards in accordance with the need of Indian capital market structure;
- to identify measures to improve cyber resilience and related business continuity and disaster recovery process in Indian securities market;
- to provide recommendations for strengthening of processes to audit cyber security and cyber resilience setups in Indian securities market;
- to periodically review the mandate and functioning of SOCs (Security Operations Centers) and to guide SEBI in setting up Cyber Lab/Cyber Center of Excellence for securities market;
- to study major cyber-attack incidents related to financial markets in domestic and global markets and identify gaps in the existing cyber security and cyber resilience framework;

- to engage in continuous dialogues with the relevant external agencies such as CERT-In (Indian Computer Emergency Response Team), National Cyber Coordination Centre (NCSC)/ National Security Council Secretariat (NSCS), Department of Telecommunications (DoT), Ministry of Electronics and Information Technology (MeitY), leading academic institutions and organisations, etc., to further strengthen cyber security and cyber resilience.

Cyber Security and Insurance Companies

Cyber security risks have equally grown as a grave concern for insurers as cyber security incidents can harm their ability to conduct business, compromise the protection of personal and proprietary data and undermine confidence in the insurance sector. Hence, it is essential to ensure that a uniform framework for information and cyber security is implemented for insurers and an in-built governance mechanism is in place within the regulated entities in order to make sure that all such security related issues are addressed from time to time.

The Insurance Regulatory and Development Authority of India (IRDAI), after a series of meetings with National Security Council Secretariat (NSCS) and several General and Life Insurance Companies in connection with reviewing cyber security status in the insurance sector, have issued guidelines to all Insurance Companies on 7 April 2017 on information and cyber security. The guidelines are applicable to all insurers and in case of intermediaries and other regulated entries with whom the policyholders' information is being shared, it would be the responsibility of insurers to ensure that adequate mechanisms are put in place to address the issues related to information and cyber security. Some of the salient features of the guidelines include:

- Appointment of Chief Information Security Officer who will be responsible for articulating and enforcing the policies to protect their information assets and formation of Information Security Committee (ISC).
- Preparation of Gap Analysis Report and formulation of Cyber Crisis Management Plan.
- Finalization of Board Approved Information and Cyber Security Policy.
- Formulation of Information and Cyber Security Assurance Programme (implementation plan/ guidelines) in line with the Board approved information and cyber security policy.
- Completion of first comprehensive information and cyber security assurance audit.

Summing-up

In a broader cyber security context, ensuring cyber security in the financial sector is a definitive step towards enhancing and fortifying security in the finance and banking domain which remains one of the core pillars of a growing and a transforming economy like ours. Cyber threats have no geographical or institutional boundaries as demonstrated in various incidents across the globe. There are significant interdependencies among the various market participants in the financial sector. In such a scenario, it is essential to have coordinated approach to tackle the menace of cyber risks and ensure that the financial stability is not endangered by economic disruptions. Moreover, it is necessary to educate people about password management and cyber security awareness. Experts have suggested the creation of a Cyber Deterrence Doctrine on the lines of India's Nuclear Deterrence Doctrine.

REFERENCES

- Government of India, Ministry of Finance, Notes/Inputs provided by the Ministry.
- Government of India, Ministry of Electronics & Information Technology, Notes/Inputs provided by the Ministry.
- Government of India, Ministry of Electronics & Information Technology, *National Cyber Security Policy 2013*.
- Ankit Sinha and Harshit Dusad, *Cyber Security in India: Need for an advanced framework,* Bar & Bench, 21 March 2017.
- Aquiles A. Almansi, *Financial Sector Cybersecurity: Who's in charge,* World Bank.
- CCG NLU Delhi, *Cybersecurity in the Financial Sector: An Overview* (http://www.legallyindia.com), 8 February 2017.
- Conference of State Bank Supervisors (CSBS), *Cybersecurity 101: A Resource Guide for Bank Executives,* Executive Leadership of Cybersecurity.
- *Cyber Security for the Financial Sector* (http://www.nccgroup.trust/uk).
- European Financial Services Round Table, *EFR Paper on Cyber security*.
- *G-7 Fundamental Elements of Cybersecurity for the Financial Sector* (http://www.ecb.europa.eu).
- Mohd. Ujaley, *Cybersecurity firms laud govt move to set up CERT for financial sector* (http://computer.expressbpd.com), 3 February 2017.
- Pankaj Maru, *What software security industry thinks of India's CERT plan for finance sector?* (http://cio.economictimes.indiatimes.com), 2 February 2017.
- Purushotham Naidu, *Dream Digital India? Let's secure our banking from cyberattacks first* (http://factordaily.com), 22 December 2016.
- Sanjiv Tomar, *National Cyber Security Policy 2013: An Assessment* (http://www.idsa.in), 26 August 2013.

Prepared by the Economic & Financial Affairs Wing of the Research & Information Division, Lok Sabha Secretariat, with inputs from the Ministries of Electronics & Information Technology and Finance and other published sources, for the use and information of the Members of Parliament.