RBI/2015-16/418
DBS.CO/CSITE/BC.11/33.01.001/2015-16

Jyeshtha 12, 1938 (saka)
June 2, 2016

To

The Chairman/ Managing Director /Chief Executive Officer
All Scheduled Commercial Banks (excluding Regional Rural Banks)

Madam / Dear Sir,

Cyber Security Framework in Banks

Introduction

Use of Information Technology by banks and their constituents has grown rapidly and is now an integral part of the operational strategies of banks. The Reserve Bank, had, provided guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (G.Gopalakrishna Committee) vide Circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011, wherein it was indicated that the measures suggested for implementation cannot be static and banks need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

2. Since then, the use of technology by banks has gained further momentum. On the other hand, the number, frequency and impact of cyber incidents / attacks have increased manifold in the recent past, more so in the case of financial sector including banks, underlining the urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cyber-security preparedness among banks on a continuous basis. In view of the low barriers to entry, evolving nature, growing scale/velocity, motivation and resourcefulness of cyber-threats to the banking system, it is essential to enhance the resilience of the banking system by improving the current defences in addressing cyber risks. These would include, but not limited to, putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions, if and when they occur.

Need for a Board approved Cyber-security Policy

3. Banks should **immediately** put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board. A confirmation in this regard may be communicated to Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision, Reserve Bank of India, Central Office, World Trade Centre-I, 4th Floor, Cuffe Parade, Mumbai 400005 at the earliest, and in any case not later than September 30, 2016.

It may be ensured that the strategy deals with the following broad aspects:

Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank

4. In order to address the need for the entire bank to contribute to a cyber-safe environment, the Cyber Security Policy should be distinct and separate from the broader IT policy / IS Security policy so that it can highlight the risks from cyber threats and the measures to address / mitigate these risks.

5. The size, systems, technological complexity, digital products, stakeholders and threat perception vary from bank to bank and hence it is important to identify the inherent risks and the controls in place to adopt appropriate cyber-security framework. While identifying and assessing the inherent risks, banks are required to reckon the technologies adopted, alignment with business and regulatory requirements, connections established, delivery channels, online / mobile products, technology services, organisational culture and internal & external threats. Depending on the level of inherent risks, the banks are required to identify their riskiness as low, moderate, high and very high or adopt any other similar categorisation. Riskiness of the business component also may be factored into while assessing the inherent risks. While evaluating the controls, Board oversight, policies, processes, cyber risk management architecture including experienced and qualified resources, training and culture, threat intelligence gathering arrangements, monitoring and analysing the threat intelligence received vis-à-vis the situation obtaining in banks, information sharing arrangements (among peer banks, with IDRBT/RBI/CERT-In), preventive, detective and corrective cyber security controls, vendor management and incident management & response are to be outlined.

Arrangement for continuous surveillance

6. Testing for vulnerabilities at reasonable intervals of time is very important. The nature of cyber-attacks are such that they can occur at any time and in a manner that may not have been anticipated. Hence, it is mandated that a SOC (Security Operations Centre) be set up at the earliest, if not yet been done. It is also essential that this Centre ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

IT architecture should be conducive to security

7. The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times. The same needs to be reviewed by the IT Sub Committee of the Board and upgraded, if required, as per their risk assessment in a phased manner. The risk cost/potential cost trade off decisions which a bank may take should be recorded in writing to enable an appropriate supervisory assessment subsequently.

8. An indicative, but not exhaustive, minimum baseline cyber security and resilience framework to be implemented by the banks is given in Annex 1. Banks should proactively initiate the process of setting up of and operationalising a Security Operations Centre (SOC) to monitor and manage cyber risks in real time. An indicative configuration of the SOC is given in Annex 2.

Comprehensively address network and database security

9. Recent incidents have highlighted the need to thoroughly review network security in every bank. In addition, it has been observed that many times connections to networks/databases are allowed for a specified period of time to facilitate some business or operational requirement. However, the same do not get closed due to oversight making the network/database vulnerable to cyber-attacks. It is essential that unauthorized access to networks and databases is not allowed and wherever permitted, these are through well-defined processes which are invariably followed. Responsibility over such networks and databases should be clearly elucidated and should invariably rest with the officials of the bank.

Ensuring Protection of customer information

10. Banks depend on technology very heavily not only in their smooth functioning but also in providing cutting-edge digital products to their consumers and in the process collect various personal and sensitive information. Banks, as owners of such data, should take appropriate steps in preserving the Confidentiality, Integrity and Availability of the same, **irrespective** of whether the data is stored/in transit within themselves or with customers or with the third party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by banks.

Cyber Crisis Management Plan

11. A Cyber Crisis Management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy. Considering the fact that cyber-risk is different from many other risks, the traditional BCP/DR arrangements may not be adequate and hence needs to be revisited keeping in view the nuances of the cyber-risk. As you may be aware, in India, CERT-IN (Computer Emergency Response Team – India, a Government entity) has been taking important initiatives in strengthening cyber-security by providing proactive & reactive services as well as guidelines, threat intelligence and assessment of preparedness of various agencies across the sectors, including the financial sector. CERT-IN also have come out with National Cyber Crisis Management Plan and Cyber Security Assessment Framework. CERT-In/NCIIPC/RBI/IDRBT guidance may be referred to while formulating the CCMP.

12. CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out. Banks are expected to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. Among other things, banks should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

Cyber security preparedness indicators

13. The adequacy of and adherence to cyber resilience framework should be assessed and measured through development of indicators to assess the level of risk/preparedness. These indicators should be used for comprehensive testing through independent compliance checks and audits carried out by qualified and

competent professionals. The awareness among the stakeholders including employees may also form a part of this assessment.

Sharing of information on cyber-security incidents with RBI

14. It is observed that banks are hesitant to share cyber-incidents faced by them. However, the experience gained globally indicates that collaboration among entities in sharing the cyber-incidents and the best practices would facilitate timely measures in containing cyber-risks. It is reiterated that banks need to report all unusual cyber-security incidents (whether they were successful or were attempts which did not fructify) to the Reserve Bank. Banks are also encouraged to actively participate in the activities of their CISOs' Forum coordinated by IDRBT and promptly report the incidents to Indian Banks – Center for Analysis of Risks and Threats (IB-CART) set up by IDRBT. Such collaborative efforts will help the banks in obtaining collective threat intelligence, timely alerts and adopting proactive cyber security measures.

Supervisory Reporting framework

15. It has been decided to collect both summary level information as well as details on information security incidents including cyber-incidents. Banks are required to report promptly the incidents, in the format given in Annex-3.

An immediate assessment of gaps in preparedness to be reported to RBI

16. The material gaps in controls may be identified early and appropriate remedial action under the active guidance and oversight of the IT Sub Committee of the Board as well as by the Board may be initiated immediately. The identified gaps, proposed measures/controls and their expected effectiveness, milestones with timelines for implementing the proposed controls/measures and measurement criteria for assessing their effectiveness including the risk assessment and risk management methodology followed by the bank/proposed by the bank, as per their self-assessment, may be submitted to the Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision, Central Office not later than July 31, 2016 by the Chief Information Security Officer.

Organisational arrangements

17. Banks should review the organisational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.

Cyber-security awareness among stakeholders / Top Management / Board

18. It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. Banks should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of the bank's cyber resilience objectives, and require and ensure appropriate action to support their synchronised implementation and testing. It is well recognised that stakeholders' (including customers, employees, partners and vendors) awareness about the potential impact of cyber-attacks helps in cyber-security preparedness of banks. Banks are required to take suitable steps in building this awareness. Concurrently, there is an urgent need to bring the Board of Directors and Top Management in banks up to speed on cyber-security related aspects, where necessary, and hence banks are advised to take immediate steps in this direction.

A copy of this circular may be placed before the Board of Directors in its ensuing meeting.

Yours sincerely,

(R.Ravikumar)
Chief General Manager
Encl: As above