भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

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

बैंकिंग पर्यवेक्षण विभाग, केंद्रीय कार्यालय, वर्ल्ड ट्रेड सेंटर, सेंटर- I, कफ परेड, कोलाबा, मुंबई -400005
Department of Banking Supervision, Central Office, World Trade Centre, Cuffe Parade, Colaba, Mumbai 400005
टेलीफ़ोन/ Tele: +91 22 22189131-39; फैक्स / Fax +91 22 22180157; ईमेल /email : cgmicdbsco@rbi.org.in

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

Annex 1

Baseline Cyber Security and Resilience Requirements

An indicative but not exhaustive list of requirements to be put in place by banks to achieve baseline cyber-security/resilience is given. This may be evaluated periodically to integrate risks that arise due to newer threats, products or processes. Important security controls for effective cyber security as may be articulated by CERT-In also may be referred. Some of the key points to be kept in mind are:

a. In view of the growing technology adoption and potential threats, the role of IT Sub-committee may be reviewed; Board level involvement and guidance would set the right tone at the top.
b. It is important to endeavour to stay ahead of the adversary.
c. Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time.
d. It is important to keep the vigil and to constantly remain alert.
e. While hardware devices and software applications may provide security, it is important to configure them appropriately.
f. Human resources are the key and ensure that they are provided with appropriate training. Communicate the security policy of the bank periodically.

Baseline Controls

1) Inventory Management of Business IT Assets

1.1 Maintain an up-to-date inventory of Assets, including business data/information including customer data/information, business applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc. indicating their business criticality. The banks may have their own framework/criteria for identifying critical assets.

1.2 Classify data/information based on information classification/sensitivity criteria of the bank

1.3 Appropriately manage and provide protection within and outside organisation borders/network taking into consideration how the data/information are stored, transmitted, processed, accessed and put to use within/outside the bank's network, and level of risk they are exposed to depending on the sensitivity of the data/information.

2) Preventing execution of unauthorised software

2.1 Maintain an up-to-date and preferably centralised inventory of authorised/unauthorised software(s). Consider implementing whitelisting of authorised applications / software/libraries, etc.

2.2 Have mechanism to centrally/otherwise control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and mechanism to block /prevent and identify installation and running of unauthorised software/applications on such devices/systems.

2.3 Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank. If a patch/series of patches is/are released by the OEM/manufacturer/vendor for protection against well-known/well publicised/reported attacks exploiting the vulnerability patched, the banks must have a mechanism to apply them expeditiously following an emergency patch management process.

2.4 Have a clearly defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).

3) Environmental Controls

3.1 Put in place appropriate environmental controls for securing location of critical assets providing protection from natural and man-made threats.

3.2 Put in place mechanisms for monitoring of breaches / compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the bank.

4) Network Management and Security

4.1 Prepare and maintain an up-to-date network architecture diagram at the organisation level including wired/wireless networks;

4.2 Maintain an up-to-date/centralised inventory of authorised devices connected to bank's network (within/outside bank's premises) and authorised devices enabling the bank's network. The bank may consider implementing solutions to automate network discovery and management.

4.3 Ensure that all the network devices are configured appropriately and periodically assess whether the configurations are appropriate to the desired level of network security;

4.4 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

4.5 Have mechanisms to identify authorised hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the bank.

4.6 Have mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.

4.7 Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

4.8 Establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

4.9 Security Operation Centre to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.

4.10 Boundary defences should be multi-layered with properly configured firewalls, proxies, DMZ perimeter networks, and network---based IPS and IDS. Mechanism to filter both inbound and outbound traffic to be put in place.

5) Secure Configuration

5.1 Document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically,

5.2 periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the bank's network including in Data Centres, in third party hosted sites, shared-infrastructure locations.

6) Application Security Life Cycle (ASLC)

6.1 Incorporate/Ensure information security across all stages of application life cycle.

6.2 In respect of critical business applications, banks may consider conducting source code audits by professionally competent personnel/service providers or have

assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.

6.3 Secure coding practices may also be implemented for internally /collaboratively developed applications.

6.4 Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.

6.5 The development, test and production environments need to be properly segregated.

6.6 Software/Application development approach should be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secure rollout.

6.7 Ensure that software/application development practices addresses the vulnerabilities based on best practices baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism.

6.8 Consider implementing measures such as installing a “containerized” apps on mobile/smart phones for exclusive business use that is encrypted and separated from other smartphone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.

6.9 Ensure that adoption of new technologies shall be adequately evaluated for existing/evolving security threats and IT/security team of the bank reach reasonable level of comfort and maturity with such technologies before introducing for critical systems of the bank.

7) Patch/Vulnerability & Change Management

7.1 Follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

7.2 Put in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.

7.3 Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto

7.4 Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.)

7.5 Periodically conduct Application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in environment closely resembling or replica of production environment.

7.6 As a threat mitigation strategy, identify the root cause of incident and apply necessary patches to plug the vulnerabilities.

7.7 Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs in the Data Centre (ii) LAN/WAN interfaces (iii) bank's network to external network and interconnections with partner, vendor and service provider networks are to be securely configured.

8) User Access Control / Management

8.1 Provide secure access to the bank's assets/services from within/outside bank's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other secure web protocols, etc.)

8.2 Carefully protect customer access credentials such as logon userid, authentication information and tokens, access profiles, etc. against leakage/attacks

8.3 Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.

8.4 Implement centralised authentication and authorisation system or accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.

8.5 Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/superuser/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).

8.6 Implement controls to minimize invalid logon counts, deactivate dormant accounts.

8.7 Monitor any abnormal change in pattern of logon.

8.8 Implement measures to control installation of software on PCs/laptops, etc.

8.9 Implement controls for remote management/wiping/locking of mobile devices including laptops, etc.

8.10 Implement measures to control use of VBA/macros in office documents, control permissible attachment types in email systems.

9) Authentication Framework for Customers

9.1 Implement authentication framework/mechanism to provide positive identify verification of bank to customers.

9.2 Customer identity information should be kept secure.

9.3 Banks should act as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

10) Secure mail and messaging systems

10.1 Implement secure mail and messaging systems, including those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

10.2 Document and implement email server specific controls

11) Vendor Risk Management

11.1 Banks shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.

11.2 Banks shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment.

11.3 Among others, banks shall regularly conduct effective due diligence, oversight and management of third party vendors/service providers & partners.

11.4 Establish appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities shall be put in place.

11.5 Banks shall ensure and demonstrate that the service provider (including another bank) adheres to all regulatory and legal requirements of the country. Banks may necessarily enter into agreement with the service provider that amongst others provides for right of audit by the bank and inspection by the regulators of the country.

11.6 Reserve Bank of India shall have access to all information resources (online/in person) that are consumed by banks, to be made accessible to RBI officials by the banks when sought, though the infrastructure/enabling resources may not physically be located in the premises of banks.

11.7 Further, banks have to adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders.

11.8 Banks shall thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the bank's critical assets.

11.9 Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third party service providers

12) Removable Media

12.1 Define and implement policy for restriction and secure use of removable media/BYOD on various types/categories of devices including but not limited to workstations/PCs/Laptops/Mobile devices/servers, etc. and secure erasure of data on such media after use.

12.2 Limit media types and information that could be transferred/copied to/from such devices.

12.3 Get the removable media scanned for malware/anti-virus prior to providing read/write access.

12.4 Consider implementing centralised policies through Active Directory or End-point management systems to whitelist/blacklist/restrict removable media use.

12.5 As default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorised for defined use and duration of use.

13) Advanced Real-time Threat Defence and Management

13.1 Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.

13.2 Implement Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralised management and monitoring.

13.3 Consider implementing whitelisting of internet websites/systems.

13.4 Consider implementing secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway

14) Anti-Phishing

14.1 Subscribe to Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications.

15) Data Leak prevention strategy

15.1 Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.

15.2 This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

15.3 Similar arrangements need to be ensured at the vendor managed facilities as well.

16) Maintenance, Monitoring, and Analysis of Audit Logs

16.1 Consult all the stakeholders before finalising the scope, frequency and storage of log collection.

16.2 Manage and analyse audit logs in a systematic manner so as to detect, understand or recover from an attack.

16.3 Enough care is to be taken to capture audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.

17) Audit Log settings

17.1 Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software , ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.

18) Vulnerability assessment and Penetration Test and Red Team Exercises

18.1 Periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems, particularly those facing the internet.

18.2 The vulnerabilities detected are to be remedied promptly in terms of the bank's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

18.3 Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams.

18.4 Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Senior/Top Management.

18.5 Red Teams may be used to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.

18.6 Periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc.

19) Incident Response & Management

Responding to Cyber-Incidents:

19.1 Put in place a fully effective Incident Response programme with due approval of the Board / Top Management.

19.2 Have written incident response procedures including the roles of staff / outsourced staff handling such incidents; Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & co-ordination with stakeholders during response;

19.3 Have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies.

Recovery from Cyber - Incidents:

19.4 Bank's BCP/DR capabilities shall adequately and effectively support the Bank's cyber resilience objectives and should be so designed to enable the bank to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.

19.5 Banks shall ensure such capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative & co-ordinated resilience testing that meet the bank's recovery time objectives.

19.6 Such testing shall also include testing of crisis communication to customers and other internal and external stakeholders, reputation management. Adequate capacity

shall be planned and maintained, in consideration thereof. The following may be considered:

(a) Define incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans.

(b) Establish and implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incidents.

(c) Establish and implement systems to collect and share threat information from local/national/international sources following legally accepted/defined means/process

(d) Document and communicate strategies to respond to advanced attacks containing ransom ware/cyber extortion, data destruction, DDOS, etc.

(e) Contain the level of cyber-attack by implementing shielding controls/quarantining the affected devices/systems.

(f) Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.

20) Risk based transaction monitoring

20.1 Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels.

20.2 The bank should notify the customer, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.

21) Metrics

21.1 Develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.

21.2 Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

22) Forensics

22.1 Have support/ arrangement for network forensics/forensic investigation/DDOS mitigation services on stand-by.

22.2 Periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc.

23) User / Employee/ Management Awareness

23.1 Define and communicate to users/employees, vendors & partners security policy/ies covering secure and acceptable use of bank's network/assets including customer information/data, educating them about cybersecurity risks and protection measures at their level.

23.2 Encourage them to report suspicious behaviour incidents to the incident management team.

23.3 Conduct targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.)

23.4 Evaluate the awareness level periodically.

23.5 Establish a mechanism for adaptive capacity building for effective Cybersecurity Management. Making cyber security awareness programs mandatory for new recruits and web-based quiz & training for lower, middle & upper management every year. (Recent and past cyber-attacks show, cyber adversaries are also targeting bank employees).

23.6 Board members may be sensitised on various technological developments and cyber security related developments periodically.

23.7 Board members may be provided with training programmes on IT Risk / Cyber-security Risk and evolving best practices in this regard so as to cover all the Board members atleast once a year.

24) Customer Education and Awareness

24.1 Improve and maintain customer awareness and education with regard to cybersecurity risks.

24.2 Encourage customers to report phishing mails/ Phishing sites and on such reporting take effective remedial action.

24.3 Educate the customers on the downside risk of sharing their login credentials / passwords etc. to any third party vendor and the consequences thereof.

Setting up and Operationalising Cyber Security Operation Centre (C-SOC)

Introduction

1 - Banking Industry in India has evolved technologically over the years and currently delivering innovative services to its customers. These services are delivered nonstop, round the clock and the customers access these services using Internet and Mobile Connectivity. Security of the financial transactions is of paramount importance and therefore the RBI has come out with guidelines from time to time addressing the security and operational aspects for specific applications and services.

2 - It is important and pertinent to look at specifically the Internet facing applications and services that are currently delivered and proposed to be delivered in the immediate future in the Banking Industry and come out with Cyber Security guidelines across the applications and services.

3 - Constant and Continuous monitoring of the environment using appropriate and cost effective technology tools, clearly defined policies and procedures based on best practices and monitored by technically competent and capable manpower is the urgent need for the Industry. Compliance to the Government guidelines that are put out periodically covering the cyber security policy, protecting critical information infrastructure and the Information Technology Act are of paramount importance. It is important to address the governance, technology, operational, outsourcing and legal issues while setting up the Cyber Security Operations Centre.

4 – Issues that need to be kept in mind while setting up the CSOC is given below. These are indicative but not exhaustive.

Governance Aspects:

- Top Management/Board Briefing on Threat Intelligence
- Dashboards and oversight
- Policy, measurement and enforcement (key metrics, reporting structure, define what is to be reported)
- Informing stakeholders , stakeholder participation

Cyber SoC: Points to be considered

1 - Conventional or Traditional Security systems have always focussed on preventive approaches over the years and are reactive in nature. They are in a position to address the concerns regarding known attacks. It is to be noted that the threat landscape has changed significantly in the recent past and therefore the approach and methodology required to be put in place has to necessarily take into account proactive approaches rather than reactive approaches and have to also address possible unknown attacks. For example, zero day attacks and attacks for which signatures are not available have to be kept in mind.

2 - The Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics.

3 - The systems that are implemented currently to monitor the security operation takes into account collection of the logs from each one of the point products deployed, storing and processing of the logs, correlation through appropriate SIEM tools, continuous monitoring of SIEM screens and finding the anomalies, if any and raising the alarms.

4 - The systems that NEED to be put in place as a part of the Cyber SoC requires the following aspects to be addressed.

- Methods to identify root cause of attacks, classify them into identified categories and come out with solutions to contain further attacks of similar types.
- Incident investigation, forensics and deep packet analysis need to be in place to achieve the above.
- Dynamic Behaviour Analysis. – preliminary static & dynamic analysis and collecting Indicators of Compromise (IOC)
- Analytics with good dash board, showing the Geo-location of the IP’s
- Counter response and Honeypot services

Expectations from SOC:

- Ability to Protect critical business and customer data/information, demonstrate compliance with internal guidelines, country regulations and laws
- Ability to Provide real-time/near-real time information on and insight into the security posture of the bank
- Ability to Effectively and Efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery
- Ability to assess threat intelligence and the proactively identify/visualize impact of threats on the bank
- Ability to know who did what, when , how and preservation of evidence
- Integration of various log types and logging options into SIEM, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customized based on risk and compliance requirements/drivers, etc.), etc.

Key Responsibilities of SOC could include:

- Monitor, analyze and escalate security incidents
- Develop Response - protect, detect, respond, recover
- Conduct Incident Management and Forensic Analysis
- Co-ordination with contact groups within the bank/external agencies

5 - Building blocks for the Cyber SoC:

TECHNOLOGY ISSUES:

First step is to arrive at a suitable and cost effective technology framework designed and implemented to ensure proactive monitoring capabilities aligned with the banking technology risk profile and business and regulatory

requirements. Clear understanding of the service delivery architecture deployed by the Bank to deliver innovative customer services will enable identification of the location for the sensors to collect the logs that are required to carry out the analysis and investigation. SIEM is able to meet this requirement to some extent but a holistic approach to problem identification and solution is required.

Second step is to have security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations with options for further deep dive investigations

Third step is to look at deep packet inspection approaches which are currently implemented using the UTM solutions that deliver wire speed performance with on the fly deep packet inspection.

Fourth step is to have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements

It is to be noted that the solution architecture deployed for the above has to address performance and scalability requirements in addition to high availability.

Need to think through by appropriately designing the

- SIEM architecture & use cases
- Log types and logging options (data sources, integration into SIEM)
- Integration of various log types and logging options into the SIEM, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customized based on risk and compliance requirements/drivers, etc.), etc.
- Technology for improving effectiveness and efficiency (tracking of metrics, analytics, scorecards, dashboards, etc.)

PROCESS RELATED ASPECTS:

One of the key aspects that require attention while designing the CSC is to understand the process to be followed to identify the root cause of a security breach and further steps to mitigate such attacks in future.

Incident Management

Problem management processes with reference to security operations Vulnerability and Patch Management Security risk management Availability management Computer forensics and response management are the key metrics that need to be well understood and architectured while configuring the solution.

PEOPLE RELATED ISSUES:

CSC is managed and monitored by competent and capable staff round the clock and therefore it is important to look at a suitable structure for this requirement.

The Level 1 monitoring by adequately trained staff working round the clock is the first step. They need to have training and product/ vendor certification to handle the tasks efficiently.

Level 2 deals with highly trained staff in specific areas of network, data security, end point security etc. to address the requirements especially while carrying out the root cause analysis as well as suitable corrective steps.

Level 3 staff are called the SoC analysts. They have profound knowledge of security, perform deep packet analysis, collection of IOC, forensic knowledge for collection of evidence, malware reverse engineering and write custom scripts whenever required.

It is to be noted that all the staff involved in the above exercise need to have a good knowledge of the products and services deployed by the respective Bank.

- Banks need to seriously consider practical ways of tackling the following issues when it comes to hiring and managing staff/people for SOC. It is not any other function in the bank. There has to be a different approach

because such personnel with required skill sets that are hard to find and retain.

- Staffing of SOC – is it required to be 24x7x365, in shifts, business hours only….etc.
- Model used - Finding staff with required skills /managed service provider with required skill set
- Training own staff/training of staff by service provider
- Appropriate compensation/incentives to retain trained staff /staff with required skill set
- Metrics to measure performance of SOC
- Ensuring scalability and continuity of staff through appropriate capacity planning initiatives

EXTERNAL INTEGRATION:

While delivering services to the customers of the Bank, several stake holders are involved directly or otherwise. They do have experience which could be very useful. For example the threat intelligence feeds from various sources may be provided by the product vendors and other major players in the technology landscape. Security information feeds from other Banks in particular and the financial ecosystem in general will be quite useful.

Cyber response cells, CERT-In and telecom service providers of the Bank may add value to the discussions based on the happenings in the Industry at large.

IDENTIFYING A SUITABLE MODEL FOR IMPLEMENTATION:

Some of the decisions which have to be taken upfront is to look at BOO or the Outsourcing model. It is difficult to reverse this decision post implementation and therefore it is important.

- Should the SoC be in-house or outsourced?
- Should it address only the Internet facing environment or the complete IT infrastructure?

- Does each Bank need to set up independently or should we look at the consortium based approach?
- Do we need to keep in mind the Bank's risk posture?

Points to keep in mind while planning for SOC in view of

(a) Specialized skill set requirements of operating and managing a SOC,

(b) Difficulty in finding experienced staff,

(c) Time consuming and expensive trainings,

(d) Designing of suitable compensation strategies,

(e) difficulty of retaining staff due to continual need for updated training, lack of adequate career path options, and overstretching ,

(f) Resource requirements pertaining to other supporting functions such as (i) system administration of systems facilitating SOC operations such as SIEM/dashboard/reporting/workflow/case management systems, etc., (ii) receiving, integrating and using threat intelligence, (iii) implementing communication strategy, (iv) Supervision/ management of SOC staff/personnel, (v) meeting compliance requirements of regulators/laws/regulations

Template for reporting Cyber Incidents

1. **Security Incident Reporting (SIR) to RBI (within two to 6 hours):**
2. **Subsequent update(s) RBI (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of RBI):**

Basic Information	
1. Particulars of Reporting:	
• Name of the bank	
• Date and Time of Reporting to RBI, CERT-IN, other agencies (please mention separately time of reporting to each)	
• Name of Person Reporting	
• Designation/Department	
• Contact details (e.g. official email-id, telephone no, mobile no)	
2. Details of Incident:	
• Date and time of incident detection	
• Type of incidents and systems affected (i) **Outage of Critical IT system(s)** (e.g. CBS, Treasury Systems, Trade finance systems, Internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT, NACH, IMPS, etc.) (ii) **Cyber Security Incident** *(e.g. DDOS, Ransom ware/crypto ware, data breach, data destruction, web*	

defacement, etc.)? ***[Please complete Annex]*** (iii) **Theft or Loss of Information** *(e.g. sensitive customer or business information stolen or missing or destroyed or corrupted)?* (iv) **Outage of Infrastructure** *(e.g. which premises-DC/Central Processing Units, branch, etc., power/utilities supply, telecommunications supply,)?* (v) **Financial** *(e.g. liquidity, bank run)?* (vi) **Unavailability of Staff** (e.g. number and percentage on loss of staff /absence of staff from work (vii) **Others** *(e.g. outsourced service providers, business partners, breach of IT Act/any other law and RBI/SEBI regulations. Etc.)?*	
• What actions or responses have been taken by the bank at the time of first reporting/till the time of subsequent reporting?	
3. Impact Assessment(examples are given but not exhaustive):	
• Business impact including availability of services – Banking Services, Internet banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement activities, etc.	

• Impact on stakeholders– affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc.	
• Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds, etc.	
• Regulatory and Legal impact	
4. Chronological order of events:	
• Date of incident, start time and duration.	
• Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
• Stakeholders informed or involved	
• Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.)	
• Rationale on the decision/activation of BCP and/or DR	
5. Root Cause Analysis(RCA):	
• Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	
• Interim measures to mitigate/resolve the issue, and reasons for taking such	

measures, and	
• Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected (one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. Date/target date of resolution_____ (DD/MM/YYYY).	
•	
•	
•	

Note: All fields are REQUIRED to be filled unless otherwise stated.

CYBER SECURITY INCIDENT REPORTING(CSIR) FORM	
General Information	**Report No:**

1. Contact Information: *(Please provide if different from what is reported in Basic Information above)*

Name of bank:

Name of the person reporting and Designation:

Department

Official Email :

Telephone/Mobile :

2. Is this a ☐New incident ☐Update to reported incident?

- For the first update, please indicate "1. If this is an update to a reported incident, please provide the update number for this update. (X.1, X.2, X.3, X.4, etc. where X is the Report No.
  Update No: Click here to enter text.

3 What severity is this incident being classified as?

Severity 1 ☐ Affected critical system(s)/ customer facing applications/systems, crippled Internal network or a combination of the above	Severity 2 ☐ Incident occurred on system or network that could put the bank's network / critical system(s) or a combination of them at risk	

Information about the Incident

4. Please indicate the date and time the incident was reported to the RBI. If it is also reported to Other Agencies (CERT-IN/NCIIP), Law enforcement agencies, separately indicate the date and time of such reporting.

(Please specify in Indian Local Time (+5.30 GMT))

Reported to RBI - Date: Click here to enter a date.

Reported to CERT-IN Date: Click here to enter a date.

Reported to NCIIP Date: Click here to enter a date.

Reported to ----mention the name of agency Date: Click here to enter a date.

5. Types of Threat/Incident

((Please select more than one, as applicable)

☐ Denial of Service (DoS) ☐ Distributed Denial of Service (DDoS)

☐ Virus/Worm/Trojan/Malware ☐ Intrusion/Hack/Unauthorised access

☐ Website Defacement ☐ Misuse of Systems/Inappropriate usage

☐ APT/0-day attack ☐ Spear phishing/Whaling/Phishing/Wishing/Social engineering attack

☐ Other: Click here to enter text.

6. Is this incident related to another incident previously reported?

Choose an item.

- If “Yes”, provide more information on how both incidents are related. Click here to enter text.
- Please provide the reference no. of the previously reported incident.

Ref no: Click here to enter text.

Incident Details

7. Please provide details of the incident in the box below.

- When was the incident first observed/sighted/detected?
  Click here to enter a date.

- How was the incident first observed/sighted/detected?
  Click here to enter text.

- Who observed?

8. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:

-Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/ networks, etc.

Click here to enter text.

What security software installed on the system currently?

If known, any TCP or UDP ports involved in the incident.

If known, provide the affected system's IP address If known, provide the attacker's IP address

Where relevant, please indicate the Operating System of the affected critical system(s): Choose an item.

- If others, kindly state the OS: Click here to enter text.

9. What is the impact of the attack? (*Tick 'one' checkbox for each column*)

Customer Service Delivery	(Loss of) Sensitive Information	Public Confidence and Reputation
☐No Impact	☐No loss	☐No Impact
☐Minor Impact	☐Minor Loss	☐Minor Impact

☐Major Impact	☐Major Loss	☐Major Impact
☐Serious Impact	☐Serious Loss	☐Serious Impact
☐Severe Impact	☐Severe Loss	☐Severe impact

10. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the bank?

Choose an item.

- If "Yes", please provide more details.

Click here to enter text.

Incident Status

11. What is/are the type(s) of follow up action(s) that has/have been taken at this time?

Click here to enter text.

12. What is the current status or resolution of this incident?

Choose an item.

If it is not resolved, what is the next course of actions?

Click here to enter text.

13. What is the earliest known date of attack or compromise? *(Tick 'checkbox' if unknown)*

(Please specify in Indian Local Time +5.30 GMT)

Date: Click here to enter a date. Unknown: ☐

14. What is the source/cause of the incident? *('NIL' OR 'NA' if unknown)*

Click here to enter text.

15. Has the incident been reported to CERT-IN/NCIIP/ any law enforcement agency/IBCART? Choose an item.

- If "Yes", specify the agency that is being reported to.

Click here to enter text..

16. Is chain of custody maintained?

17. Has the bank filled chain of custody form?

18. What tools were used for collecting the evidence for the incident?

: Attack Vectors

E1. Did the bank locate/identify IP addresses**, domain names, related to the incident**

Whether the Indicators of Compromise, list of IP addresses identified from the incident, involvement of the IP addresses in the incident (ex. Victim, Malware Command & Control Servers, etc.), domain names resolved, involvement of the domain names in the incident. (ex. Drive-by-download Servers, Malware Control & Command Servers, defaced website), email addresses identified and their involvement, malicious files/attachments (file name, size, MD5/SHA1 hash, etc.) etc. have been reported in IB-CART/CERT-IN/NCIIP/Law enforcement agencies
