भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

RBI/2018-19/63
DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 October 19, 2018

To,
The Chairman/Managing Director/Chief Executive Officer
All Primary (Urban) Co-operative Banks

Madam/Dear Sir,

Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs)

Use of Information Technology by banks has grown rapidly and is now an important part of the operational strategy of banks. 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. There is an urgent need to put in place a robust cyber security/resilience framework at UCBs to ensure adequate security of their assets on a continuous basis. It has, therefore, become essential to enhance the security of the UCBs from cyber threats by improving the current defences in addressing cyber risks.

2. It is observed that the level of technology adoption is also different across the banks in this sector – some banks offering state of the art digital products to its customers and some banks maintaining their books of account in a standalone computer and using e-mail for communicating with its customers/supervisors/other banks. Hence, it has been decided to issue basic cyber security guidelines applicable to **all** UCBs. However, any UCB, depending on its Self-Risk Assessment, complexity of its Information Technology (IT)/ Information Security (IS) systems, nature of digital products offered, etc. is free to adopt advanced cyber security norms as decided by their Boards.

3. An indicative but not exhaustive, basic cyber security framework to be implemented by all the UCBs is given in **Annex I.**

4. Need for a Board approved Cyber Security Policy –

All UCBs should immediately put in place a Cyber Security policy, duly approved by their Board/Administrator, giving a framework and the strategy containing a suitable approach to check cyber threats depending on the level of complexity of business and acceptable levels of risk. On completion of the process of policy formulation by the Board, a confirmation shall be sent to Department of Co-operative Bank Supervision, Central Office, C-9, 1st Floor, BKC, Mumbai – 400051 by email within three months from the date of circular. It shall be ensured that the cyber security policy deals with the following broad aspects, keeping in view the level of technology adoption and digital products offered to the customers:

4.1. Cyber Security Policy to be distinct from the IT policy/IS Policy of the UCB

The Cyber Security Policy should be distinct from the IT/IS policy of the UCB so that it highlights the risks from cyber threats and the measures to address/reduce these risks. While identifying and assessing the inherent risks, UCBs should keep in view the technologies[1] adopted, delivery channels[2], digital products[3] being offered, internal[4] and external[5] threats etc., and rate each of these risks as Low, Medium, High and Very High.

4.2. IT Architecture/Framework should be security compliant

The IT architecture/ framework which includes network, server, database and application, end user systems, etc., should take care of security measures at all times and this should be reviewed by the Board or IT Sub-committee of the Board periodically. For this purpose, UCBs may carry out the following steps:

i. Identify weak/vulnerable areas in IT systems and processes,

[1] Technologies: Security incident event management (SIEM), Privilege Identity Management (PIM), database activity monitoring, etc.

[2] Delivery channels: ATM, PoS, IMPS, etc.

[3] Digital products: m-Banking, UPI, e-Wallet, etc.

[4] Internal threats: Critical & sensitive data compromise, password theft, internal source code review, etc.

[5] External threat: DDoS, Ransomware, etc.

ii. Allow restricted access to networks, databases and applications wherever permitted, through well-defined processes and approvals including rationale for permitting such access,

iii. Assess the cost of impact in case of breaches/failures in these areas and,

iv. Put in place suitable Cyber Security System to address them,

v. Specify and document clearly the responsibility for each of above steps.

A proper record should be kept of the entire process to enable supervisory assessment.

4.3. Cyber Crisis Management Plan

4.3.1 Since cyber risk is different from many other risks, the traditional BCP/DR (Business Continuity Plan/Disaster Recovery) arrangements may not be adequate and hence needs to be revisited keeping in view the nature of cyber risk. A Government of India organisation, CERT-In (Computer Emergency Response Team – India, a Government entity) has been taking important initiatives in strengthening Cyber Security by providing proactive/reactive services and guidelines, threat intelligence and assessment of preparedness of various agencies in different sectors, including the financial sector. CERT-In also has come out with National Cyber Crisis Management Plan and Cyber Security Assessment Framework. UCBs may refer to CERT-In/NCIIPC/RBI/IDRBT guidelines as reference material for their guidance.

4.3.2 UCBs should promptly detect any cyber intrusions (unauthorised entries) so as to respond/recover/contain impact of cyber-attacks. Among other things, UCBs, especially those offering services such as internet banking, mobile banking, mobile wallet, RTGS/NEFT/IMPS, SWIFT, debit cards, credit cards etc., should take necessary detective and corrective measures/steps to address various types of cyber threats[6] viz. denial of service (DoS), distributed denial of services (DDoS), ransomware/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.

[6] Refer Annex II for a brief description on the various type of threats

5. Organisational Arrangements

UCBs should review the organisational arrangements so that the security concerns are brought to the notice of suitable/concerned officials to enable quick action.

6. Cyber Security awareness among Top Management/Board/other concerned parties

Managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness/familiarisation among staff at all levels including Board and Top Management. UCBs should actively promote among their customers, vendors, service providers and other concerned parties an understanding of its cyber security objectives. Security awareness among customers, employees, vendors, service providers, etc. about the potential impact of cyber-attacks helps in cyber security preparedness of UCBs.

7. Ensuring protection of customer information

UCBs, as owners of customer sensitive 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 the third party vendors; the confidentiality of such custodial information should not be compromised in any situation. To achieve this, suitable systems and processes across the data/information lifecycle need to be put in place by UCBs. As regards customers, UCBs may educate and create awareness among them with regard to cyber security risks.

8. Supervisory reporting framework

UCBs should report immediately all unusual cyber security incidents (whether they were successful or mere attempts) to Department of Co-operative Bank Supervision, Central Office, C-9, 1st Floor, BKC, Mumbai – 400051 by email, giving full details of the incident. A ‘NIL’ report shall be submitted on quarterly basis in case of no cyber security incidents.

9. A copy of this circular shall be placed before the Board of Directors/Administrator in its ensuing meeting and a policy on Cyber Security should be framed by the Board/Administrator immediately. After framing of the policy, UCBs are advised to implement basic Cyber Security Controls as indicated in Annex I and report the same to respective Regional Offices of Department of Co-operative Bank Supervision on or before March 31, 2019.

Yours faithfully,

(Ranjeev Shanker)
(General Manager In - Charge)

Enclosed:

Annex I: Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs)

Annex II: Description of some of the cyber security threats

Annex I

Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs)

1) **Inventory Management of Business IT Assets**

   1.1 UCBs should maintain an up-to-date business IT Asset Inventory Register containing the following fields, as a minimum:

   a. Details of the IT Asset (viz., hardware/software/network devices, key personnel, services, etc.)

   b. Details of systems where customer data are stored

   c. Associated business applications, if any

   d. Criticality of the IT asset (For example, High/Medium/Low)

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

   1.3 Appropriately manage and provide protection within and outside UCB/network, keeping in mind how the data/information is stored, transmitted, processed, accessed and put to use within/outside the UCB's network, and level of risk they are exposed to depending on the sensitivity of the data/information

2) **Preventing access of unauthorised software**

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

   2.2 Put in place a mechanism to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. Also, put in place a mechanism to block/prevent and identify installation and running of unauthorised software/applications on such devices/systems.

   2.3 The web browser settings should be set to auto update and consider disabling scripts like JavaScript, Java and ActiveX controls when they are not in use.

   2.4 Internet usage, if any, should be restricted to identified standalone computer(s) in the branch of a UCB which are strictly separate from the systems identified for running day to day business.

3) **Environmental Controls**

3.1 Put in place appropriate controls for securing physical location of critical assets (as identified by the UCB under its inventory of IT 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 UCB.

4) **Network Management and Security**

4.1 Ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.

4.2 The default passwords of all the network devices/systems should be changed after installation.

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

4.4 Critical infrastructure of UCB (viz., NEFT, RTGS, SWIFT, CBS, ATM infrastructure) should be designed with adequate network separation controls

5) **Secure Configuration**

5.1 The firewall configurations should be set to the highest security level and evaluation of critical device (such as firewall, network switches, security devices, etc.) configurations should be done periodically.

5.2 Systems such as Network, application, database and servers should be used dedicatedly for the purpose for which they have been set up.

6) **Anti-virus and Patch Management**

6.1 Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software running at the systems used by the UCB officials (end-users).

6.2 Implement and update antivirus protection for all servers and applicable end points preferably through a centralised system.

7) User Access Control / Management

7.1 Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a ‘need to know’ and ‘need to do’ basis.

7.2 Passwords should be set as complex and lengthy and users should not use same passwords for all the applications/systems/devices.

7.3 Remote Desktop Protocol (RDP) which allows others to access the computer remotely over a network or over the internet should be always disabled and should be enabled only with the approval of the authorised officer of the UCB. Logs for such remote access shall be enabled and monitored for suspicious activities

7.4 Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (servers/databases, applications, network devices etc.)

8) Secure mail and messaging systems

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

8.2 Document and implement email server specific controls.

9) Removable Media

9.1 As a 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.

9.2 Secure the usage of removable media on workstations/PCs/Laptops, etc. and secure erasure/ deletion of data on such media after use

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

10) User/Employee/Management Awareness

10.1 Communicate to users/employees, vendors & partners security policies covering secure and acceptable use of UCB’s network/assets including customer information/data, educating them about cyber security risks and protection measures at their level.

10.2 Conduct awareness/training for staff on basic information security controls (Do’s and Don’ts), incident reporting, etc.

10.3 Board members may be kept updated on basic tenets/principles of IT risk/cyber security risk at least once a year.

10.4 The end-users should be made aware to never open or download an email attachment from unknown sources

11) Customer Education and Awareness

11.1 Improve and maintain customer awareness and education with regard to cyber security risks

11.2 Educate the customers on keeping their card, PIN etc. secure and not to share with any third party

12) Backup and Restoration

Take periodic back up of the important data and store this data ‘off line’ (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files).

13) Vendor/Outsourcing Risk Management

13.1 All the outsourcing service level agreements (SLAs) signed with the vendors must clearly mention the responsibility of the UCB and vendor in case of any failure of services

13.2 The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints

13.3 Vendors’ service level agreements shall be periodically reviewed for performance in security controls

----------------X----------------

Annex II

Description of some of the cyber security threats

1) Denial of service attack: A denial-of-service attack (DoS attack) generally consists of the concerted efforts of a person/persons to prevent an internet site or service from functioning efficiently. A DoS attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.

2) Distributed denial of service: In a distributed denial-of-service (DDoS) attack, large numbers of compromised systems (sometimes called a Bot net) attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby, denying the service of the system to legitimate users.

3) Ransom ware: Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

4) Malware: Malware is the term for maliciously crafted software code. Special computer programmes now exist that enable intruders to fool an individual into believing that traditional security is protecting him during online banking transactions. Attacks involving malware are a factor in online financial crime.

5) Phishing: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

6) Spear phishing: Phishing attempts directed at specific individuals or companies have been termed spear phishing. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success.

7) Whaling: The term whaling has been coined for spear phishing attacks directed specifically at senior executives and other high-profile targets. In these cases, the content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email may be an executive issue such as a subpoena or customer complaint.

8) Vishing: Vishing is the illegal access of data via voice over Internet Protocol (VoIP). Vishing is IP telephony’s version of phishing and uses voice messages to steal identities and financial resources. The term is a combination of ‘voice’ and ‘phishing’.

9) Drive-by downloads: Drive-by download means two things, each concerning the unintended download of computer software from the Internet:

a. Downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically

b. Any download that happens without a person's knowledge, often a computer virus, spyware, malware or crimeware.

10) Browser Gateway frauds: The information sent and received from a PC/device is routed through an undesired path on the network thereby exposing it to unauthorised entity. The only gateway to outside world for the PC/device being the browser that has been compromised.

11) Ghost administrator exploit: A ghost administrator exploit is a code that takes advantage of a software vulnerability or security flaw to gain Administrator’s rights/privileges in the system. This exploit allows the attacker to mask his identity in order to remotely access a network and gain Administrator rights/privileges, or move deeper into the network. In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor viruses and/or spyware to steal user information from the infected systems.

The list is an indicative list of cyber threats.