THE ARYA VAISHYA CO-OPERATIVE BANK LTD., HUBLI

CYBER SECURITY POLICY

INDEX

Para No.	Description	Page No.
1	Introduction	2
2	Level of technology adopted by the bank	3
3	IT Architecture/Framework of the Cyber security policy	3
4	Cyber Security awareness among top management/Board members/other concerned	4
5	Ensuring protection of customer information	5
6	Inventory Management of Business IT Asset and risk categorisation	5
7	Preventing execution of unauthorised software	5
8	Environmental Controls	6
9	Network Management and Security	6
10	Secure Configuration	6
11	Anti-virus, Patch Management and other best practices	7
12	User Access Control / Management	7
13	Secure mail and messaging systems	8
14	Baseline Cyber Security and Resilience Requirements - Level I	8
15	Vendor/Outsourcing Risk Management	9
16	Cyber Security controls for Third party ATM Switch Application Service Providers	10
17	Removable Media erasure	10
18	User/Employee/Management Awareness/Training	10
19	Customer Education and Awareness	11
20	Backup and Restoration	11
21	Staff accountability	11
22	Security audit and assessment	11
23	Review of cyber security policy	11
24	Supervisory reporting frameworks	11
25	Description of some of the cyber security threats	11
	Annexue-A	12

THE ARYA VAISHYA CO-OPERATIVE BANK LTD., HUBLI

CYBER SECURITY POLICY

1. Introduction

The financial sector in general and banks in particular plays a crucial role in the socio-economic progress of India. In the recent times, the financial sector has become increasingly dependent on the Information and Communication Technology (ICT), offering new and innovative delivery channels for customers.There is a noticeable shift in the banking industry in the way customers deal with their transactions. There is a rapid increase in the usage of digital channels such as internet banking, digital wallets, mobile banking, ATM. This leads to the increase in exposure and thereby cyber-attacks which further may lead to financial and reputational losses. Customer expectation is driving further changes in the way in which banks operate and offer various products. Cyber-attacks and malicious cyber activities in the banking sector -

- **i.** Causes the potential of loss of money tothe customer and/or bank,
- **ii.** Affects institution's reputation, impacts the economybesides creating trust deficit.
- **iii.** Bank may lose the customer's confidence which can further increase the impact

Cyber insecurity is the flip side of the digital revolution. As the traditional universal banking model unbundles at the hands of technology players, it is creating many opportunities for banks to engage with their customers in new ways or cater to their needs with new, innovative solutions. But it is also opening up the industry's wings to all kinds of online attack. A great example of this is the risk of banking accounts being compromised because the social media accounts they are linked to have been breached. 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.

The key influencers which makes it imperative for the banks to invest in securityto avoid cyber threats are

- **i.** Increase in financial data losses including card data
- **ii.** Personal identifiable information etc.
- **iii.** Unauthorized access to bank's network and systems

Bank should take concrete steps/measures to address such potentialthreats and take measures to protect the interest of thecustomers as well as theirsystems keeping in view the guidelines issued by RBI from time to time. Accordingly,TheAryaVaishya Co-operative Bank Ltd., Hublihasalso decidedto put in place a robust cyber security/resilience framework to ensure adequate security of its assets on a continuous basis.The Cyber Security Policy has been preparedquite distinct from the IT/IS policy of the bank keeping in view the technologies adopted, delivery channels, digital products being offered, internal and external threats etc.; so that it highlights the risks from cyber threats and the measures to address/reduce these risks and is effective irrespective of the underlying technology and products.

2. Level of technology adopted by the bank

The AryaVaishya Co-operative Bank Ltd., Hublimaintainsits books of account in an accounting software installed by MINDMILL SOFTWARE., The software enables required access conditions to conduct the desired transactions and using e-mail/fax/phone for communicating with its customers/ supervisors/ other banks.

The bank is also providing services of digital transactions like NEFT/RTGS(ShamraoVithal Co-operative Bank Ltd., Hubli Branch-Sponsor Bank)through Corporate Net Banking. As far as CTS clearing is concerned the bank is a sub member of the IDBI Bank and cheques received by 11.30 am are submitted to IDBI on the same day in respect of outward clearing. As far as inward clearing is concerned, the bank is receiving the images of the cheques from IDBI bank and after ensuring the validity of the instruments received necessary entries are posted thereafter. The bank should ensure to reconcile the account on day to day basis maintained with IDBI bank. The bank is also Core Banking Solutions (CBS) enabled and services for which has been outsourced from Mindmill Software.

3. IT Architecture/Framework of the Cyber security policy.

The IT architecture/ framework of the policy includes network, server, database,application and end user systems etc., which takes care of security measures at all times and the same is to be reviewed by the Board/IT Sub-committee of the Board periodically. In order to ensure that security measures are in place the bank should put in place following measures.

i. As mentioned in para 2 regarding the level of technology prevalent in the bank, the officers/employees operating the system should ensure that while executing the transactions for NEFT/RTGS, the details mentioned in the requisition form are entered properly so that no loss

is caused to the Bank. E mails can carry spam or malevolent software (for example worms, bugs etc.). In order to avoid virus infection or data theft, the employee should ensure to-

- Abstain from opening attachments or clicking any links in the situations when its content is not well explained.
- Make sure to always check email addresses and names of senders.
- Be careful with click bait titles (for example offering prizes, advice, etc.)
- In case that an employee is not sure if the email received, or any type of data is safe, they can always contact our IT specialist.

ii. The designated officers/employees will only have access to network, database and applications. Such designated officers will not share the user ID and password with any other officer/employee of the bank or outsider.

iii. The designated persons will meticulously follow the concept of maker and checker while executing the transactions.

iv. The data base in cloud and Disaster Recovery is managed by the CBS vender (Mindmill Software). The DR drill is conducted on quarterly basis by them for data safety. The Bank should confirm in writing the date of DR drill conducted by CBS vender.

v. The bank should promptly detect any cyber intrusion so as to respond/recover/contain impact of cyber-attack.

vi. As the bank is offering services like-RTGS/NEFT, CTS clearing etc, it should take necessary corrective steps to address various type of cyber threats such as denial of services (DoS) , distributed denial of services (DDoS) , ransom ware, business e-mail frauds including spam email phishing, browser gate way frauds pass word related frauds etc.

4. Cyber Security awareness among top management/Board members/other concerned

As per the industry assessment, internal actors are responsible for 43 percent of data loss. Half of this is intentional—disgruntled or opportunistic employees, contractors, or suppliers performing deliberate acts of data theft. But half of it is simply negligence. Employees don't want to change their password every month if they can stick with "password123" forever. Some of them probably don't see the problem while downloading the attachment from suspicious "urgent" email.

Managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This needs a high level of awareness/familiarisation among staff at all levels including Board and Top Management. Accordingly, the

board members, officers/employees of the bank should be briefed by the System administrator/consultant regarding the risk involved with the adoption of technology and various safeguards to be taken in this regard. It should be ensured that they understand the relevant details, what they are expected to do, how to do it and what could be the consequences if they don't. The bank should also advise suitably to its customers, vendors, service providers and other concerned parties an understanding of its cyber security objectives. Such awareness among customers, employees, vendors, service providers, etc. about the potential impact of cyber-attacks will help in cyber security preparedness of the bank which in turn will help avoiding cyber threats.

5. Ensuring protection of customer information

The bank will ensure preserving the Confidentiality, Integrity and Availability of the customer data, irrespective of whether the data is stored/in transit within themselves or with the third party vendors; the confidentiality of such custodial information will not be compromised in any situation. The bank will not part with any information relating to customer data without his written consent or required by the law of the land. Data transfer is one of the most common wayscybercrimes happen. The bank will follow the following best practices when transferring data:

- Avoid transferring personal data such as customer's and employee's confidential data.
- Adhere to personal data protection law.
- Data can only be shared over banks network.
- Even when working remotely, all the cyber security policies and procedures must be followed.

6. Inventory Management of Business IT Assets and risk categorisation

The bank will maintain an up-to-date business IT Asset Inventory Register containing the following fields indicating criticality of IT assets (For example, High/Medium/Low)

i. Details of the IT Asset (viz., hardware/software/network devices, key personnel, services, etc.)
The bank keeping in view the cyber threats has decided to classify details of hardware as **'low risk'** whereas details of software/network devices are to be classified under '**medium risk'.**

ii. Details of systems where customer data are stored. (To be classified under **high risk**.)

7. Preventing execution of unauthorized software

i. The bank shouldmaintain an up-to-date inventory of authorized software(s)/approved applications/software etc.

ii. The bank should not allow installation of software/application on end-user PCs, laptops, workstations, servers, mobile devices, etc. and also ensure to block/prevent and identify installation and running of unauthorised software/applications on such devices/systems. To deviate from this the concerned officers/employees have to take prior written permission of the CEO of the bank.

iii. The bank should ensure that the web browser settings are set to auto update.

iv. The bank will ensure that internet usage, if any, will be restricted to identify standalone computer(s) in the branches of the bank which are strictly separate from the systems identified for running day to day business. An inventory to this effect has to be maintained by the bank.

8. Environmental Controls

i. The bank should ensure the safety of the critical assets (as identified by the bank under its inventory of IT assets), by securing physical location to provide protection from natural and man-made threats.

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

9. Network Management and Security

i. The bank will ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.

ii. The bank will ensure that default passwords of all the network devices/systems are changed after installation.

iii. Bank should put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems. The pass word of the network should be kept confidential.

iv. The bank must prepare and maintain up-to-date network architecture diagram including wired/wireless networks.

10. Secure Configuration

i. 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.

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

11.Anti-virus, Patch Management and other best practices

i. The bank will ensure to 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 bank officials (end-users).

ii. The bank will ensure to implement and update antivirus protection for all servers and applicable end points.

iii. Besides, the bank will follow the following best practices-

- To Keep all electronic devices' password secured and protected
- Logging into bank's accounts should be done only through safe networks
- To install security updates on a regular basis.
- Not to leave your devices unprotected and exposed.
- Ensure to lock computers when leaving the desk.

12. User Access Control / Management

The bank will ensure to implement the following user accesscontrol.

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

ii. Passwords should be set as complex and lengthy and users should not use same passwords for all the applications/systems/devices to ensure avoiding that the bank account password gets hacked, use these best practices for setting up passwords:

- At least 8 characters (must contain capital and lower-case letters, numbers and symbols).
- Do not write down password and leave it unprotected.
- Do not exchange credentials when not requested or approved by supervisor.
- Change passwords every month.

iii. 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 CEO. Logs for such remote access shall be enabled and monitored for suspicious activities.As far as The AryaVaishya Co-operative Bank Ltd., Hubliis concerned, the CBS software is hosted on an application server and it is accessed through this mode only. No other third party remote desktop

license / software/ protocol is used for the purpose. Support for CBS software is provided over Team viewer by Mindmill Software., support team.

iv. Implement controls to minimize invalid log on counts, deactivate dormant accounts.

v. Monitor any abnormal change in pattern of logins.

13. Secure mail and messaging systems

The bank will ensure that 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., are in place.

14.Baseline Cyber Security and Resilience Requirements - Level I

As advised by RBI vide Circular DOS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019, the bank will implement the following Baseline Cyber Security and Resilience Requirements - Level I is applicable to the bank.

To Implement bank specific email domains (example, XYZ bank with mail domain xyz.in) with anti-phishing and anti-malware, DMARC controls enforced at the email solution. Domain-based Message Authentication, Reporting and Conformance (DMARC) is an increasingly important approach for helping ensure the integrity of email coming from a given domain. This important email security standard should be turned on by default for every domain, at every web host or every email server.

i. To put in place two factor authentication for accessing its CBS and applications connecting to the CBS with the 2nd factor being **dynamic** in nature. (Eg: 2nd factor should not be a static password and must not be associated with the PC/terminal used for putting through payment transactions)

ii. To conduct security review of PCs/terminals used for accessing corporate Internet Banking applications of ShamraoVithal Co-operative Bank LTD., CBS servers and network perimeter through a qualified information security auditor during the course of IS audit.

iii. To follow a robust password management policy as per policy of the bank and RBI guidelines, with specific emphasis for sensitive activities like accessing critical systems, putting through financial transactions. Usage of trivial passwords shall be avoided. [An illustrative but not exhaustive list of practices that should be strictly avoided are: For example, AVCB @123 as password, network/server/security

solution devices with passwords as device/solution_name123/device _name/solution@123; hard coding of passwords in plain text in thick clients or storage of passwords in plain text in the databases]

iv. To educate employees to strictly avoid clicking any links received via email (to prevent phishing attacks) by organising training programmes on the subject

v. To put in place an effective mechanism to report the cyber security incidents in a timely manner and take appropriate action to mitigate the incident. Bank shall also report all unusual cyber security incidents to CERT-In* and IB-CART#.

***The Indian Computer Emergency Response Team (*CERT*-In) is an office within the Ministry of Electronics and Information Technology. It is the nodal agency to deal with cyber security threats like hacking and phishing. It strengthens security-related defense of the Indian Internet domain.**

#Indian Banks – Center for Analysis of Risks and Threats (IB-CART). The Reserve Bank of India's Working Group on Information Security, Electronic Banking (IDRBT)

15. Vendor/Outsourcing Risk Management

In order to ensure vendor/outsourcing risk management, the bank will take care to implement the instructions issued by RBI vide circular UBD.CO.BPD.No.31/09.18.300/2013-14 dated October 17, 2013 and Circular DOS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019 as enumerated below :

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

ii. The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints. Bank shall ensure and demonstrate that the service provider (including another bank) adheres to all regulatory and legal requirement of the country

iii. Vendors' service level agreements shall be periodically reviewed for performance in security controls.

iv. Ensure appropriate management and assurance on security risks in outsourced vendor arrangements. Bank shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment. Bank shall regularly conduct effective due

diligence, oversight and management of third party vendors/service providers and partners.

v. Necessarily enter into agreement with the service provider that, among other things, provides for right to audit by the bank. The outsourcing agreements should include clauses to recognise the right of the Reserve Bank to cause an inspection to be made of a service provider of the bank and allow the Reserve Bank of India or persons authorised by it to access the bank's documents, records of transactions, logs and other necessary information given to, stored or processed by the service provider within a reasonable time.

16. Cyber Security controls for Third party ATM Switch Application Service Providers

Presently the bank is not availing ATM Switch ecosystem facility through any third party ATM Switch Application Service Providers (ASPs). However, in future as and when any such facility will be availed by the bank, it will ensure that the contract agreement signed between it and the third party ATM Switch ASP shall necessarily mandate the third party ATM Switch ASP to comply with the prescribed cyber security controls on an ongoing basis and to provide access to the RBI for on-site/off-site supervision.. It may be mentioned that these controls are applicable to the ASPs limited to the IT ecosystem (such as physical infrastructure, hardware, software, reconciliation system, network interfaces, security solutions, hardware security module, middleware, associated people, processes, systems, data, information, etc.,) providing ATM switch services as well as any other type of payment system related services to the bank.

17. Removable Media erasure

i. As a default rule, use of removable devices and media should not be permitted in the bank unless specifically authorised for defined use and duration of use.

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

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

iv. The removable media for back up should be stored off-site.

18. User/Employee/Management Awareness/Training

i. The bank will conduct awareness/training for staff on basic information security controls (Do's and Don'ts), incident reporting, etc.

ii. Board members will be kept updated on basic tenets/principles of IT risk/cyber security risk at periodical intervals.

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

19.Customer Education and Awareness

The bank will take the following measures to create awareness among the customers regarding cyber security threats.

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

ii. Encourage customers to report phishing mails, phishing sites and on such reporting take effective remedial measures.

20.Backup and Restoration

As the backup of the data is stored by the CBS vendor, DR drill should be done periodically by them and bank should ascertain the same in writing from the vendor.

21.Staff accountability

In case of breaches that are intentional or repeated, and are harmful to the bank, the management of the bank will take disciplinary actions in progressive manner depending on how serious the breach is.

22.Security audit and assessment

The bank will advise the IS auditor to mention any violations regarding cyber security policy and incorporate his assessment in the report

23. Review of cyber security policy

The bank will review its cyber security policy on annual basis keeping in view the pace of technology taking place in the banking sector and adopted by the bank.

24. Supervisory reporting frameworks

Bank 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. No report is required to be submitted in case of NIL cyber security incidents as per annexure-I to RBI Circular DOS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019.

25.Description of some of the cyber security threats

Description of some of the cyber security threats are mentioned in **Annexure-I.**

Annexure I
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: Ransom ware is a type of malicious software from crypto virology 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, Active X component, or Java applet) automatically
b. Any download that happens without a person's knowledge, often a computer virus, spyware, malware or crime ware.

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 unauthorized entity. Theonly 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.

Hubli.

Date :30/05/2024 G. Manager Director Director Chairman