ROYAL MONETARY AUTHORITY OF BHUTAN

RMA/DIT/Cybersecurity/1819/5857

Date:2/4/2019

The Chief Executive Officer
All Member Banks

Subject: Directives on Cybersecurity Framework Implementation

Dear Sir,

As banks continue to advance towards digitilisation and adoption of online digital financial services—both domestic and international, the banks are faced with the unprecedented challenges of cyber-security breaches, which have increased significantly; hence the need for the banks to implement a robust cyber-security framework is crucial to enhance the resilience of our banking system to address unknown and advanced cyber-threats with the view to protect and benefit both customers and the banks.

Given the increasing popularity of domestic digital payments, cross-border acceptance of RuPay card and the banks international cards witnessing significant rise—such as Visa and MasterCard, and fund transfer using SWIFT network, the level of interdependency and interconnectedness with these digital ecosystems have, in turn, exposed the diversity of external cyber-threats for cyber-criminals to target and exploit, which can cause systemic issue, reputational damage and financial loss.

In the wake of emerging incidents of cyber-threats gaining prominence and towards strengthening the cyber-security posture of our payment and financial infrastructure in a coordinated and integrated approach, the member banks should put in place a robust cyber-security framework as outlined below, including developing sound practices and cyber-security controls to increase effectiveness in response to cyber-attacks, as prescribed in Annexure 1:

1. Implementing EMV at the ATMs and PoS terminals

Currently, the ATMs and PoS terminals of all the member banks in the country accepts and processes only magnetic strip-based cards. Consequently, both ATM and PoS based card transactions continue to remain highly vulnerable to skimming or cloning, including other fraudulent activities. Therefore, it has become essential to transition all ATMs and PoS terminals to EMV compliant, to reduce card-present fraud by enhancing the safety and security of transactions. Further, the EMV requirement will also ensure and align the member banks preparedness for the in-effect EMV "Liability Shift," effective 1st January 2019, for RuPay PoS and ATMs transactions. Due to variations in ATM and PoS hardware and EMV application kernel requirements, the banks should account for this variability and plan for the migration with the vendors and service providers at the earliest.

POST BOX:154,CHHOPHEL LAM, KAWAJANGSA, THIMPHU BHUTAN
TEL# :(+975-2-323110, 323111, 323112, 321699) FAX :(+975-2-322847)
SWIFT:RMABBTBT

2. Replacing magnetic strip-based cards with EMV chip and PIN based cards

The increasing usage of magnetic stripe credit and debit cards at various digital access points has witnessed the upsurge in the frauds due to the cards being stolen, data being compromised and cards counterfeiting, making it easier preys for the fraudsters to copy the data from these cards. Against this backdrop, the member banks are directed to replace existing magnetic strip with EMV chip and PIN based cards, by employing dynamic authentications, to further enhance the security and risk mitigation in card-present transactions by shielding user data from unauthorized access.

3. Cybersecurity measures and responses: PCI-DSS and ISO 27001

With the rising volume and complexity of cyber attacks plaguing the businesses, largely targeted to exploit the banks and its customers due to attractiveness of financial gain and access to confidential financial data, there is no doubt that cyber attacks pose a serious threat to the stability of the overall financial sector. In this regard, the banks need to proactively respond to combatting cyber crime by reviewing measures and undertaking what more could be done to identify, address and mitigate threats to overall financial stability. In this respect, the Royal Monetary Authority undertook to assess security vulnerabilities and to improve its cyber security preparedness through successful award of PCI-DSS (Payment Card Industry Data Security Standard) and ISO 27001:2013 (Information Security Management Systems) certifications. Along the same vein, the Authority would mandate all member banks to work towards assessing PCI-DSS compliance aimed at protecting their Cardholder Data Environment (CDE). Further, the banks may consider implementing ISO 27001:2013 assessment to further complement and extend the overall cyber security measures.

4. Formation of a Financial Institutions Cyber Response Team (FICRT)

Given our shared responsibilities to contribute towards building cyber-resilience, there is a need to put in place an information sharing platforms, such as formation of Financial Institutions Cyber Response Team, to encourage banks in cooperation with the RMA to promote active collaboration and effective information sharing pertaining to cyber-security. In particular, the FICRT will play a crucial role in facilitating and exchange of cyber security issues and offer lessons-learned advice and expertise that would benefit from working together. The team will actively monitor cyber security threats, to plan for and coordinate counter-threat measures to prevent the types of cyber security risks, apart from reporting the incidents to the supervisors or authorities as soon as possible. Additionally, the platform will serve to train cyber experts through training and education programs on effective cyber practices and assessments, which could help make the financial system more resilient.

5. Implement basic cybersecurity controls and measures

As an immediate measure to ascertain that basic information security and cyber secure practices are established in the banking infrastructure relating to people, process and technology, the banks should implement the right cyber security controls and responsive actions indicated in the ***Annexure I***. These controls, although not exhaustive, are expected to further strengthen the current security controls in banks environment and additionally, assist in complying with PCI DSS/ ISO 27001:2013 Certification requirements.

As we continue to adapt to the new digital future, the Royal Monetary Authority would encourage all the banks to comply with the aforementioned cyber-security mandates and develop comprehensive and forward-looking approach, including through simulation exercises and penetration testing. A quarterly progress report must be provided by all member banks to the Authority underscoring the progress to cyber-security due diligence aimed at building cyber-resilience across the financial system.

Following the issuance of this letter, the Department of Information Technology, RMA will organize a meeting with the Heads of IT of the Financial Institutions to follow-up and support, where necessary.

Yours sincerely,

(Dasho Penjore)
Governor

Annexure I

Basic Cyber Security Controls Framework for Member Banks

1. Inventory Management of Critical IT Assets

1.1. All banks should maintain an accurate and up-to-date IT Asset Inventory Register containing the following fields, as a minimum:

a. Details of the IT Asset (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)

e. Software implemented

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

1.3. Appropriately manage and provide protection within and outside bank/network, keeping in mind how the data/information is 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 installation/use of unauthorized software

2.1. Maintain an up-to-date and preferably centralized inventory of authorized software(s)/approved applications/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. and mechanism to block/prevent and identify installation and running of unauthorized software/applications on such devices/systems.

2.3. Ensure that only licensed software/ applications are installed in the servers/ end user devices.

2.4. Internet usage should be restricted to identified standalone computer(s) in the bank which are strictly separate from the systems identified for running day to day business.

3. Environmental Controls

3.1. Implement appropriate controls for securing physical location/access to critical assets (as identified by the banks under its inventory of IT assets), providing protection from natural

and man-made threats. Permit only authorized access to critical infrastructure such as Data Center and all entry/exit should be logged and monitored.

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.

4. Network Management and Security

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

4.2. All default passwords of the network devices/systems must 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 banks (ATM Switch, CBS, GIFT, SWIFT, ATM infrastructure) should be designed with adequate network segregation controls.

4.5. Only access to required ports and services for business need must be provided which must be periodically assessed and reviewed.

4.6. Conduct quarterly Vulnerability Assessment on the critical banking systems, network devices, servers and penetration testing at least annually or after any significant change in infrastructure or configuration.

5. Secure Configuration

5.1. The firewall configurations must be set to highest security and evaluation of critical device configurations (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.

5.3. Ensure that the servers, network devices, security devices, etc. are hardened as per standards and best practices.

6. Anti-virus and Patch Management

6.1. Put in place systems or 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 staff (end-users).

6.2. Implement and update endpoint antivirus protection for all servers and end user computers preferably through a centralized system.

7. User Access Control / Management

7.1. Disable/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. Configure Active Directory Server with domain administration rights and include end user computers to be a part of the central domain server.

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

7.4. Implement appropriate (e.g. centralized) 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 that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

8.2. Implement secure practices such as 2-step verification for mail logins.

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 authorized 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 bank'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 management/ 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

12.1. 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 bank and vendor in case of any failure of services

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

14. Information Security Policy (ISP)

14.1. Draft and implement an Information Security Policy document which outlines all the aforementioned controls and additional relevant procedures for strict adherence by all staff of the organization.

15. Information Security Steering Committee (ISSC)

15.1. Form an Information Security Steering Committee (ISSC) that shall act as an oversight committee to govern, advise and ensure compliance to the security mandates.

15.2. ISSC shall appoint the Information Security Officer (ISO) who is responsible for articulating and enforcing the policies that banks use to protect their information assets apart from coordinating the security related issues / implementation within the organization as well as relevant external agencies.

**********************End of document**********************