भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

SEBI/HO/MIRSD/CIR/P/2017/0000000100
September 08, 2017

To,

Registrars to an Issue / Share Transfer Agents

Dear Sir/Madam,

Subject: Cyber Security and Cyber Resilience framework for Registrars to an Issue / Share Transfer Agents (hereinafter referred to as RTAs)

Rapid technological developments in securities market have highlighted the need for maintaining robust cyber security and cyber resilience framework to protect the integrity of data and guard against breaches of privacy.

A robust cyber security and cyber resilience framework should identify the plausible sources of operational risk, both internal and external, and mitigate the impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of its obligation in the event of cyber attack.

Since RTAs perform important functions in providing services to holders of securities, it is desirable that RTAs have robust cyber security and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

In view of the above, SEBI's High Powered Steering Committee - Cyber Security engaged in detailed discussions and decided that the framework prescribed vide SEBI circular CIR/MRD/DP13/2015 dated July 06, 2015 on cyber security and cyber resilience framework be broadly made applicable for large RTAs. Accordingly, the provisions of this circular are applicable only for RTAs servicing more than 2 crore folios (hereinafter referred to as "Qualified RTAs" or "QRTAs"). The framework placed at Annexure A, would be required to be complied by the QRTAs with regard to cyber security and cyber resilience. QRTAs are directed to take necessary steps to put in place systems for implementation of this circular, by December 01, 2017.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully,

Debashis Bandyopadhyay
General Manager

Annexure A

1. Cyber attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber security framework includes measures, tools and processes that are intended to prevent cyber attacks and improve cyber resilience. Cyber Resilience is an organisation's ability to prepare and respond to a cyber attack and to continue operation during, and recover from, a cyber attack.

Governance

2. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber attacks and threats, QRTAs should formulate a comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board of QRTAs, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the Board of QRTAs atleast annually with the view to strengthen and improve its cyber security and cyber resilience framework.

3. The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risk associated with processes, information, networks and systems;

   a. 'Identify' critical IT assets and risks associated with such assets,
   b. 'Protect' assets by deploying suitable controls, tools and measures,
   c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes,
   d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack,
   e. 'Recover' from incident through incident management, disaster recovery and business continuity framework.

4. The Cyber security policy should encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research

Organisation (NTRO), Government of India, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

5. QRTAs should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

6. QRTAs should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the QRTAs.

7. The Board of the QRTAs shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a quarterly basis review the implementation of the cyber security and cyber resilience policy approved by their Board, and such review should include review of their current IT and cyber security and cyber resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience. The review shall be placed before the Board of the QRTAs for appropriate action.

8. QRTAs should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.

9. The aforementioned committee and the senior management of the QRTAs, including the CISO, should periodically review instances of cyber attacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.

10. QRTAs should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have access or use systems / networks of QRTA's, towards ensuring the goal of cyber security.

Identify

11. QRTAs should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, QRTAs should maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

12. QRTAs should accordingly identify cyber risks (threats and vulnerabilities) that it may face, alongwith the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

13. QRTAs should also encourage its third-party providers, if any, to have similar standards of Information Security.

Protection

Access Controls

14. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.

15. Any access to QRTA's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. QRTAs should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

16. QRTAs should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.

17. QRTAs should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.

18. QRTAs should deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

19. Account access lock policies after failure attempts should be implemented for all accounts.

20. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorised access to the QRTA's critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.

21. Two-factor authentication at log-in should be implemented for all users that connect using online/internet facility.

22. QRTAs should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc.

23. Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical security

24. Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorised employees.

25. Physical access to the critical systems should be revoked immediately if the same is no longer required.

26. QRTAs should ensure that the perimeter of the critical equipments room are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

27. QRTAs should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. The QRTAs should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

28. QRTAs should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT infrastructure from security exposures originating from internal and external sources.

29. Anti-virus software should be installed on servers and other computer systems. Updation of anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

Security of Data

30. Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA-2, etc.

31. QRTAs should implement measures to prevent unauthorised access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

32. The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.

33. QRTAs should allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

34. Only a hardened and vetted hardware / software should be deployed by the QRTAs. During the hardening process, QRTAs should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments / software.

35. All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

Application Security and Testing

36. QRTAs should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

Patch Management

37. QRTAs should establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

38. QRTAs should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of systems and storage devices

39. QRTAs should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

40. QRTAs should regularly conduct vulnerability assessment to detect security vulnerabilities in the IT environment. QRTAs should also carry out periodic penetration tests, atleast once in a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

41. Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

42. In addition, QRTAs should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces.

Monitoring and Detection

43. QRTAs should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised

copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.

44. Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, QRTAs should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.

45. Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

Response and Recovery

46. Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident.

47. The response and recovery plan of the QRTAs should aim at timely restoration of systems affected by incidents of cyber attacks or breaches. QRTAs should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.

48. The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber attacks or breach of cyber security mechanism.

49. Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

50. QRTAs should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

51. Quarterly reports containing information on cyber attacks and threats experienced by QRTAs and measures taken to mitigate vulnerabilities, threats and attacks including

information on bugs / vulnerabilities / threats that may be useful for other QRTAs should be submitted to SEBI in soft copy to rta@sebi.gov.in

52. Such details as are felt useful for sharing with other QRTAs in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

53. QRTAs should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines.

54. The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Periodic Audit

55. QRTAs shall arrange to have its systems audited on an annual basis by an independent CISA/CISM qualified or equivalent auditor to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board of QRTAs within three months of the end of the financial year.