भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MRD/TPD/P/CIR/2023/146 **August 29, 2023**

To,

All Stock Exchanges,
All Clearing Corporations,
All Depositories

Sir/ Madam,

Subject: - Guidelines for MIIs regarding Cyber security and Cyber resilience

1. Market Infrastructure Institutions (i.e. Stock Exchanges, Clearing Corporations and Depositories) are systemically important institutions as they, *inter-alia*, provide infrastructure necessary for the smooth and uninterrupted functioning of the securities market. As part of the operational risk management, these Market Infrastructure Institutions (MIIs) need to have robust cyber security framework to provide essential facilities and perform systemically critical functions relating to trading, clearing and settlement in securities market. It is also important that MIIs establish and continuously improve their Information Technology(IT) processes and controls to preserve confidentiality, integrity and availability of data and IT systems.

2. With the change in market dynamics in the Indian Securities markets, the interdependence among the MIIs has seen significant increase. Considering the interconnectedness and interdependency of the MIIs to carry out their functions, the cyber risk of any given MII is no longer limited to the MII's owned or controlled systems, networks and assets.

3. In view of the above, based on the recommendations of the High Powered Steering Committee on Cyber Security of SEBI and in consultation with MIIs, it has been decided to issue guidelines for strengthening the existing cyber security and cyber resilience framework of MIIs. The said guidelines are placed at **Annexure-A** and MIIs are required to comply with the same.

4. These guidelines should be read in conjunction with the applicable SEBI circulars (including but not limited to that relating to Cybersecurity and Cyber Resilience

framework, System and Network Audit framework, etc.) and subsequent updates issued by SEBI from time to time.

5. The compliance of the guidelines shall be provided by the MIIs along with their cybersecurity audit report (conducted as per the applicable SEBI Cybersecurity and Cyber Resilience framework). The compliance shall be submitted as per the existing reporting mechanism.

6. The provisions of the Circular shall come into force with immediate effect.

7. MIIs are required to take necessary steps to put in place systems for implementation of the circular, including necessary amendments to the relevant bye-laws, rules and regulations, if any, within 120 days from the date of the circular.

8. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 , read with Regulation 51 of the Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018 and Section 19 of the Depositories Act, 1996 read with Regulation 97 of Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

9. The circular is issued with the approval of Competent Authority.

10. This circular is available on SEBI website at www.sebi.gov.in under the category “Legal” and dropdown “Circulars”.

Yours faithfully,

Ansuman Dev Pradhan
Deputy General Manager
+91-22-26449622
ansumanp@sebi.gov.in

Annexure-A

MIIs are required to implement the following practices: -

1) MIIs shall maintain offline, encrypted backups of data and shall regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity and availability

2) MIIs shall maintain regularly updated “gold images” of critical systems in the event they need to be rebuilt. This entails maintaining image “templates” that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.

3) MIIs should explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in the event starting MII’s operations from both Primary Data Centre (PDC) and Disaster Recovery Site (DRS) are not feasible. The MIIs should also try to keep spare hardware in ready to use state for delivering critical services and such systems shall be updated as and when new changes (for example OS patches, security patches) are implemented in the primary systems. This spare hardware should regularly undergo testing in line with response and recovery plan of the MIIs.

4) MIIs should undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level to deal with the ransomware attacks. One such drill scenario recommended to be tested is recovering from ransomware attack considering both PDC and DRS have been impacted. This would assess the effectiveness of people, process and technologies to deal with such attacks.

5) MIIs should conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

6) MIIs should patch and update software and OSs to the latest available versions and it must be reviewed on a quarterly basis to ensure the implementation of the same.

7) MIIs should implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g. phishing) or incidents.

8) MIIs should implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses, malicious domains/URLs at the firewall.

9) MIIs should ensure Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP), antivirus and anti-malware software and signatures are up to date on all IT systems.

10) MIIs should use application directory whitelisting on all assets to ensure that only authorized software is run and all unauthorized software is blocked from installations/executing.

11) MIIs should employ Multi Factor Authentication(MFA) for all services.

12) MIIs should apply the principle of least privilege to all the systems and services so that users have the access to the jobs they need to perform along with solutions like Privileged Identity Management (PIM)/ Privileged Access Management (PAM) in place.

13) MIIs should put in place configuration management database approach to.-

    a) Understand and inventorise their IT assets, both logical (e.g., data, software) and physical (e.g., hardware).

    b) Understand which data or systems are most critical for providing critical services, as well as any associated interdependencies (i.e., “critical asset or system list”).

14) MIIs shall regularly review the Active Directory (AD) to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target for attackers.

15) Secure domain controllers (DCs)- Threat actors often target and use DCs as a staging point to spread ransomware network-wide.

a) MIIs should ensure that DCs are patched as and when patch is released and it must be reviewed on a quarterly basis to ensure the implementation of the same.
b) MIIs should ensure that no unnecessary software is installed on DCs, as these can be leveraged to run arbitrary code on the system.
c) MIIs should ensure that access to DCs should be restricted to the Administrators group- Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
d) MIIs should ensure that DC host firewalls are configured to prevent direct internet access.
e) MIIs shall undertake the penetration testing activity (internal and external) for known Active Directory Domain Controller abuse attacks. Weaknesses shall be remediated on topmost priority.

16) Delegated access and unused tokens should be reviewed and cleaned at least on quarterly basis.

17) MIIs should retain and adequately secure logs for security devices, applications, databases, operating systems, servers, public facing servers hosted on clouds, end points and network devices etc., with full verbosity.

18) Network devices of MIIs should also be configured in line with whitelist approach including IPs, ports and services for inbound and outbound communication with proper Access Control List (ACL) implementation.

19) MIIs should build effective network segregation for containing cyber incidents and minimizing disruption to business operations.

20) MIIs should ensure secure usage of RDP (Remote Desktop Protocol) in IT systems. Further, it must be implemented on need to use basis only and it must employ MFA (Multi Factor Authentication) service. Remote access, if necessary, should be given to authorised personnel from whitelisted IP for predefined time period only with a provision to log all activities.

21) Connecting to MIIs via Application Programming Interface(API) should be strictly on whitelisting approach. MIIs should have API security solution in place for securing services and data transferred through APIs.

22) MIIs should implement Domain name system (DNS) filtering services to ensure clean DNS traffic is allowed in the environment. Domain name system security extensions (DNS-Sec) for secure communication shall be used.

23) Management of the critical servers / applications / services / network elements should only be restricted through enterprise identified intranet systems.

24) MIIs should have system(s) in place to manage and incorporate IOCs /malware alert/vulnerability-alert (received from CERT-in or NCIIPC or any linked MII or any other government agency) in their systems.

25) MIIs shall devise standard operating procedure (SoP) to implement the advisories issued by CERT-In, NCIIPC or any other government agency in their IT environment within defined timeframe and the said SoP shall be shared with SEBI.

26) MII's response and recovery plan should be subjected to review and testing. Tests should address an appropriate broad scope of scenarios including simulation of extreme but plausible cyber-attacks. Tests should be designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. These tests must include the critical service provider, vendors and linked MIIs.

27) MIIs should explore the possibility of running the systems on dissimilar/different application architecture in order to ensure the high availability in the event of disaster.

28) MIIs should engage Dark Web monitoring services to check for any brand abuse, data/ credential leak etc.