SEBI released Cyber Security & Cyber Resilience Framework for Stock Brokers/ Depository Participants
Last Updated On: June 23, 2020, 8:27 p.m.

# CYBERSECURITY AND CYBER RESILIENCE FRAMEWORK FOR STOCK BROKERS/ DEPOSITORY PARTICIPANTS

Stockbrokers and depository participants perform important functions in providing services to holders of securities, it is beneficial that these entities have robust cybersecurity and cyber resilience framework in order to provide essential facilities and perform systemically critical functions related to the securities market.

Accordingly, After discussions with Exchanges, Depositories, and Stock Brokers and Depository Participants associations, a framework on cyber security and cyber resilience has been designed.

Operational risk management framework to manage risk to systems, networks, and databases from cyber-attacks and threats, Stock Brokers/ Depository Participants should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework.

## Stock Brokers and depositors shall;

- make necessary amendments related to byelaws, rules and regulations for the implementation of the above direction;
- bring the provisions to the notice of their members/participants and also publish the same on their websites;
- Communicate to SEBI regarding the status of implementation of the provisions in their Monthly Report.

## SEBI has directed all the concerned on subject vide their Circular no. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018, to build a strong focus on Cyber Security and recovery process. The directions require:

- DP to prepare comprehensive – annual review in Board meeting
- Make a senior designated officer
- Half yearly review by Internal technology committee
- Define the responsibilities of vendors, employees outsource staff etc..
- Identify cyber risks and control measures.

## The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks, and systems:

- 'Identify' critical IT assets and risks associated with such assets.

- 'Protect' assets by deploying suitable controls, tools and measures.
- 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes.
- Respond' by taking immediate steps after identification of the incident, anomaly or attack.
- 'Recover' from incident through incident management and other appropriate recovery mechanism

## GOVERNANCE:

- Stock Brokers / Depository Participants should appoint a senior official or management personnel i.e a Designated Officer
- The Designated Officer whose function would be to assess, identify, and reduce security and 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 Policy.
- The Stock Brokers / Depository participants shall constitute an internal Technology Committee comprising experts.
- This Technology on a half-yearly basis should review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board.
- Stock Brokers / Depository Participants should establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.

## IDENTIFICATION:

- Stock Brokers / Depository Participants should identify critical assets based on their sensitivity and criticality for business operations, services, and data management. Stock Brokers / Depository Participants should maintain up to date inventory of its hardware and systems and the personnel to whom these have been issued, Software and information assets both internal and external details of its network resources, connections to its network, and data flows.
- Stock Brokers / Depository Participants should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

## PROTECTION:

1. **Access control**

- Two-factor security
- A user access log of at least 2 years
- Review access of privileged users
- Access deactivation of people leaving the organization

2. **Physical Security**

- Access to critical systems – restriction – accompanied by staff
- Use of Security Guard, CCTV, cards, etc.

3. **Network Security Management**

- Establish Baseline standards, secured LAN and wireless networks
- Measures for servers running algorithmic trading applications
- Network security devices such as Firewalls, proxy servers, IDS
- Controls for Virus/malware/ransomware attack

4. **Data Security**

- Identification of critical data – use of strong encryption for data in motion
- Control over open ports

5. **Application security in customer-facing applications**

- Application authentication security, password policies, two factor authentications

6. **Certification of off-the-shelf products**

- Standardization Testing and Quality Certification, intensive regression testing, configuration testing, etc.

7. **Patch Management**

- Patch management procedures including identification, categorization, and prioritization of patches and updates
- Rigorous testing procedures of patches before deployment

8. **Disposal of data, systems and storage devices**

- Suitable policy including crypto shedding, degauss or such other procedures
- Data disposal and data retention policy

9. **Vulnerability Assessment and Penetration Testing (VAPT)**

- Conduct assessment and detect security vulnerabilities
- Penetration testing of services available over internet
- Reporting of gaps and remedial actions

10. **Monitoring and detection**

- Monitoring security events, alerts and timely detection of unauthorized activities, changes, copying or transmission of data
- Ensuring high resilience, high availability, and detection of attacks on system exposed over internet

11. **Response and recovery**

- Response to alerts received to prevent the expansion of incident, mitigation and eradication of incident
- Restoration plan according to SEBI circulars
- Defined roles and responsibilities

12. **Sharing of information**

- Quarterly reporting of cyber issues to Stock exchanges / SEBI within 15 days from the end of quarter

13. Training and education

- Make staff aware of IT issues, increasing awareness, focus on non-technical staff

14. The system managed by vendors

- Adherence to Cyber security policy and self-certifications

## Periodic Audit requirement

The Depositories and stockbrokers have implemented IT related policies from 1st April 2019. The systems need to be audited by CERT-IN empanelled auditor or in independent CISA/CISM qualified auditor on an annual basis. The report so issued by him will have a detailed check on certain areas and management comments on non-compliance areas.

## Conclusion:

In the world of uncertainties, growing cyber risks is very important and essential it's high time that all the organizations design and maintain internal controls with the best of business practices. This will always add value to the business and will have a long run where we can see uninterrupted business growth.