

Document Name	CSE Cyber Security and Cyber Resilience Policy
Document Creation Date	22/08/2015
Document Created By	DGM-ITD
Version Control History	1.7
Document Reviewed Date	05/12/2024
Document Reviewed By	CISO-CSE & CRO-CSE
Document Approved By	Standing Committee on Technology

CSE Cyber Security and Cyber Resilience Policy

Overview

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases. This Cyber Security Policy is a formal set of rules defined by The Calcutta stock Exchange Ltd. (CSE) and all the users of CSE IT resources must abide by this policy.

Purpose

The Cyber Security Policy serves several purposes. The main purpose is to inform users: employees, vendors and other authorized users of their obligatory requirements for protecting the technology and information assets of The Calcutta Stock Exchange Ltd. The Cyber Security Policy describes the technology and information assets that its users must protect and identifies many of the threats to those assets.

Scope

The scope of this policy includes all those people who are given access to The Calcutta Stock Exchange Ltd (CSE) and its wholly owned subsidiary CSE Capital Markets Private Limited (CCMPL) systems to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the CSE are made up of the following components:

1. Computer hardware resources like servers, storage, networking equipment (router, switch, firewall, hubs, modem etc.), PCs (desktops & laptops) and mobile devices.
2. System software including operating systems, database management systems, backup & restoration software, integrated communication & security software of different networking devices etc.
3. Application software used for trading purposes by various department/users of CSE & CCMPL.
4. Utility/Security software like antivirus software, network management software (NMS) & different other software tools.

Policy

1. As per the cyber security and cyber resilience policy, the following process is to be followed 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.
2. The senior officer in IT department having knowledge in Networking and Cyber Security, will act 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 for implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the CSE.

3. The Oversight Standing Committee on Technology of the CSE will review on a quarterly basis the implementation of the cyber security and resilience policy approved by their Boards, and such review should include review of their current IT and cyber security and resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience
4. A reporting procedure has to be established to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.
5. The aforementioned committee and the senior management, including the CISO, will periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.
6. 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 CSE, towards ensuring the goal of cyber security should be defined.

Identify

Critical assets based on their sensitivity and criticality for business operations, services and data management has to be identified. To this end, an 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 have to be maintained. Possible risk and their countermeasures need to be identified on periodic basis as a part of continual improvement.

Review should be done every 3-5 years to assess the requirement for upgrade of critical IT assets/resources of CSE environment to mitigate risks using latest technologies.

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 have also to be identified.

Third-party providers, such as service providers, stock brokers, depository participants, etc. will be encouraged to have similar standards of Information Security.

Protection Access Controls

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

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

Strong password controls have to be implemented 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 and the user credential data has to be stored using strong and latest hashing algorithms as per the password policy of the Exchange.

User access are uniquely identified and logged in system for audit and review purposes. Such logs have to be maintained in read-only format and stored in encrypted form for a period not less than 2 years.

Additional controls and security measures have to be deployed to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures will 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.

Account access lock policies after failure attempts have to be implemented for all accounts.

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

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

An Internet access policy has to be formulated to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc.

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

Physical security

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 authorized employees.

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

It has to be ensured that the perimeter of the critical equipment's 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

Baseline standards has to be used to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. Regular enforcement checks has to be conducted to ensure that the baseline standards are applied uniformly.

Network security devices, such as firewalls as well as intrusion detection and prevention process has to be installed to protect its IT infrastructure from security exposures originating from internal and external sources.

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 preferably through automatic deployment of latest pattern files and engines to all the clients through a Central Antivirus Control Unit.

Security of Data

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.

Measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity should be implemented. It should be ensured that confidentiality

of information is not compromised during the process of exchanging and transferring information with external parties.

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.

Only authorized data storage devices should be allowed through appropriate validation processes. Proper data leak prevention technologies may be deployed and configured properly at different layers in the network to secure all business sensitive data.

Hardening of Hardware and Software

Only a hardened and vetted hardware / software should be deployed. During the hardening process, default passwords are replaced with strong passwords and all unnecessary services and protocols are removed or disabled in equipment / software.

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. Hardening procedure for individual assets should be drafted based on world-wide accepted standards/guidelines like CIS (Centre for Internet Security).

Application Security and Testing

Regression testing like uncovering software bugs, enhancements, patches and new configuration should be undertaken before implementation. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions. Testing should be conducted on periodic basis and as well as on requirement/on-demand basis.

Patch Management

The patch management procedures should be established to include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

Rigorous testing of security patches should be performed before deployment into the production environment so as to ensure that the applications of patches do not impact other systems.

Rollback plan has to be formulated, reviewed and approved before implementing patches. Backups should be taken before and after any major change/critical patch.

Disposal of systems and storage devices

CSE 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)

Vulnerability assessment should be carried out on periodic basis to detect security vulnerabilities in the IT environment. Periodic penetration tests should also be done, at least 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. Apart from periodic VAPT, on demand VAPT needs to be conducted based on specific requirement.

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

In addition, perform vulnerability scanning and conduct penetration testing to be done prior to the commissioning of a new system, which offers Internet accessibility and open network interfaces.

VAPT is conducted in all the critically important CSE and CCMPL servers.

Monitoring and Detection

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

Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, suitable mechanism has to be implemented to monitor capacity utilization of its critical systems and networks.

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

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.

The response and recovery plan should aim at timely restoration of systems affected by incidents of cyber-attacks or breaches. The recovery plan should be in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified by SEBI.

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.

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.

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

Sharing of information

Quarterly reports containing information on cyber-attacks and threats experienced by CSE and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful to other Exchanges, should be submitted to SEBI. Such details as are felt useful for sharing with other Exchanges in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

Periodic training programs will have to be conducted 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.

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

Periodic Audit

The Terms of Reference for the System Audit of CSE specified vide circular CIR/MRD/DMS/13/2011 dated November 29, 2011 accordingly modified to include audit of implementation of the aforementioned areas.

Also as a part of statutory audit procedure CSE audits the iBOS system every year.

CSE and CCMPL also conducts Cyber Security and Resilience Audit for NSE & BSE based trading systems and NSDL & CDSL DP operations every year as per SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019

Version Control History

Version Change Date: 03/11/2022

Version Number: 1.5

Changes:

- Under the topic '**Overview**' the second sentence may be restructured as follows:
"This Cyber Security Policy is a formal set of rules defined by CSE and all the users of CSE IT resources must abide by this policy."
- Under the topic '**Scope**' the points 1-4 re-structured as follows:
 1. Computer hardware resources like servers, storage, networking equipment (router, switch, firewall, hubs, modem etc.), PCs (desktops & laptops) and mobile devices.
 2. System software including operating systems, database management systems, backup & restoration software, integrated communication & security software of different networking devices etc.
 3. Application software used for trading purposes by various department/users of CSE.
 4. Utility/Security software like antivirus software, network management software (NMS) & different other software tools.
- Under the topic '**Policy**', the following changes have been made:
 - a. Under Point 1., "the following process" added in the first line.
 - b. Under point 2, the word "and" in the clause 'establishment and implementation' in the fourth line, may be replaced with the word "for".
 - c. Under the topic '**Identify**', the following line added at the end of paragraph 1: Possible risk and their countermeasures need to be identified on periodic basis as a part of continual improvement.
 - d. Review should be done every 3-5 years to assess the requirement for upgrade of critical IT assets/resources of CSE environment to mitigate risks using latest technologies.
- Under the topic '**Protection Access Controls**', in paragraph 4, the clause "Such logs have to be maintained and stored" replaced with the clause "Such logs have to be maintained in read-only format and stored". A new section Centralized Anti-Virus Management has been added with all its processes
- Under the topic '**Network Security Management**' in paragraph 3, the clause "preferably through automatic deployment of latest pattern files and engines to all the clients through a Central Antivirus Control Unit.", added after the words "regular basis".
- Under the topic '**Security of Data**' the following line added at the end: Proper data leak prevention technologies may be deployed and configured properly at different layers in the network to secure all business sensitive data.
- Under the topic '**Hardening of Hardware and Software**', the words "and protocols" added after the word "services" in the second line. Hardening procedure for individual assets should be drafted based on world-wide accepted standards/guidelines like CIS (Centre for Internet Security).
- Under the topic '**Application Security and Testing**', the following sentence should be added at the end: Testing should be conducted on periodic basis and as well as on requirement/on-demand basis.
- Under the topic '**Patch Management**' the following sentences has been added at the end:
Rollback plan has to be formulated, reviewed and approved before implementing patches.
Backups should be taken before and after any major change/critical patch
- Under the topic '**VAPT**', in the first line, the words "regular basis" is replaced by the words "periodic basis". At the end of paragraph one, the following has been added:
Apart from periodic VAPT, on demand VAPT needs to be conducted based on the requirement

Version Change Date: 17/05/2023

Version Number: 1.6

Changes:

- Under the topic 'Scope' the sentence 'and its wholly owned subsidiary CSE Capital Markets Private Limited (CCMPL)' has been added.
- Also the in the 3rd point of scope CCMPL has been added too
- The last paragraph of the Periodic Audit has been added as 'CSE and CCMPL also conducts Cyber Security and Resilience Audit for NSE & BSE based trading systems and NSDL & CDSL DP operations every year as per SEBI Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 and SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019'.
- In the VAPT section this line has been added 'VAPT is conducted in all the critically important CSE and CCMPL servers'.

Version Change Date: 05/12/2024

Version Number: 1.7

Changes:

- Specific name of CISO has been removed and new reviewer (CRO-CSE) has been added.