CHOICE EQUITY BROKING PVT. LTD

Crisis Management Plan

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	11-Jan-20	1.5	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	15-July-21	1.6	Sunil Utekar	Yogesh Jadhav
Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav
Reviewed On	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj

Table of Contents

1. Purpose

The purpose of this plan is to enable Choice Equity Broking Pvt. Ltd. (Choice) to recover effectively and efficiently in the event of a security crisis. The plan shall establish a response structure, which shall comprise representation from key stakeholders.

2. Scope

In situations of crisis that leads to adverse consequences like downtime of applications, systems or non- availability of critical business units and services, the Crisis Management Plan shall serve as governing document to handle the crisis.

3. Crisis Definition

Crisis is an escalated information or cyber security incident which breaches the manageable threshold impact of an incident, impacting Choice Equity Broker Pvt. Ltd. (Choice) revenue, data loss, availability, customer and internal users.

4. Crisis Identification Criteria

Post security incident classification, perform preliminary analysis to decide if the event is a potential crisis. Security incidents that may result into one more of the below mentioned criteria shall be classified as a crisis.

Sr.	Parameter	Measurement
1	Data Loss	Choice Equity Broking Pvt. Ltd. (Choice)'s confidential data
2	Availability impact	of more than 30 mins (business working hours) for: a critical customer interfacing application; or a critical business unit; or a substantial number of firm's employees are affected that impairs business
3	Customer Impact	Customer related details
4	Internal Users Impacted	Critical departments/ users

The Crisis Handler shall identify potential crisis situations and notify CISO. The CISO shall discuss the business impact with the Crisis Response Team. Upon consensus, the identified incidents maybe declared as crisis.

5. Crisis Response Team

The Crisis Response Team shall monitor the crisis and suggest remedial steps to be taken to mitigate and resolve the crisis.

5.1 Team Members

i. COO
ii. CISO
iii. Legal & Compliance Head
iv. Communications Head
v. Respective Business CTO, depending upon crisis

5.2 Roles & Responsibilities

a. Crisis Response Team:
- Take decision to invoke Crisis Management Plan
- Facilitate communication with various departments during crisis
- Create a team for crisis resolution based on the nature of crisis that has been declared
- Identifying and allocating skillful resources to handle crisis
- Define extent of investigation during a crisis
- Convene periodically to discuss the effectiveness of the Crisis Management Plan
- Based on the nature of the crisis co-ordinate with various regulators / governing bodies / agencies such as CERT-In, RBI, etc.
- Provision for external assistance if the internal teams cannot handle the crisis

b. Chief Information Security Officer (CISO)
- Consult with CTO and invoke crisis based on preliminary understanding of the incident
- Facilitate and lead discussions amongst various departments and Senior Management during crisis
- Review decisions and activities executed by the Crisis Handler
- Provide guidance on activities to be undertaken as a part of forensic activities
- Supervise the recovery operations being carried out
- Ensure that CMP is updated periodically to reflect the changing business and technology landscape
- Improve security controls, security policy and crisis management plan based on learnings from post crisis activities

c. Information Security Working Group
- Monitor the infected assets post crisis resolution for any anomalies
- Update as required, the Information Security Policy and Procedures, Incident Management Policy and Procedure, Business Continuity and Disaster Recovery Plan and Crisis Management Plan, based on lessons learnt.

d. Crisis Handler
   - Lead the Technology, Business Services in conducting forensic and mitigation investigation of the crisis
   - Identify duration and types of logs to be analyzed during the crisis
   - Ensure that logs and evidence being captured is following the Digital Evidence Handling Guidelines (Refer: Incident Management Procedure)
   - Communicate the scope and activities to be undertaken as a part of forensic activities to the Technology, Business Services
   - Identify compromised systems by performing root cause analysis and notify the relevant teams
   - Define containment strategy in consultation with CISO
   - Formulate recovery strategy based on the type of incidents
   - Ensure all decisions being taken and actions being performed are recorded for future analysis and knowledge management
   - Present preliminary status report of the crisis to the Crisis Response Team
   - Notify the Crisis Response Team of resolution of the crisis
   - Activate the war room

e. Technology/ Business Services including any third parties/vendors
   - Perform forensic activities as communicated by the Crisis Handler
   - Assist the Crisis Handler to identify compromised systems and containment actions
   - Extract all logs that are relevant to the crisis
   - Isolate/contain compromised systems as informed by the Crisis Handler
   - Perform recovery activities as per the recovery strategy adopted
   - Based on lessons learnt from the crisis, enhance the technology infrastructure to avoid such crisis situations in the future

f. Business Team
   - Conduct initial business impact assessment due to crisis
   - Periodically monitor any drastic fluctuations to the initial impact assessment report during the crisis
   - Decide on recovery strategy including invocation of BCP/DR

g. BCP/DR Team
   - Invoke BCP/DR, for resolution of the crisis, if required

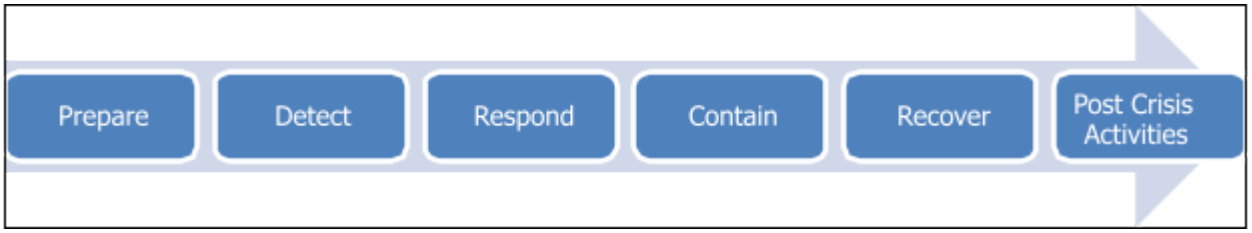
h. Communications Team
   - Consult Crisis Response Team and formulate official statements regarding the crisis
   - Communicate as required with the media and other broadcasting channels

i. Legal & Compliance Team
   - Ensure compliance with all national, international and state laws and regulations are followed during a crisis
   - Report to the relevant regulatory body

- Inform the Crisis Response Team regarding whether the evidence is admissible when taking action; specifying how evidence can be collected; third-party maintenance liability exposure
- Assist the Senior Management to understand the legal implications of the crisis
- Provide inputs for any media releases/regulatory filings being made
- Provide inputs for acquisition, handling and storage of digital evidence according to all national, international and state laws and regulations

6. Crisis Response Methodology

The various stages involved in the crisis management lifecycle are: -



A. Prepare

Choice Equity Broking Pvt. Ltd. (Choice) shall implement appropriate security controls to prevent an information or cyber incident from escalating to a crisis. Some of the appropriate measures include:

Hardening of infrastructure

Monitoring of infrastructure and logs

Vulnerability assessments and penetration testing exercises

Forensic readiness

Cyber simulation exercises such as DDoS simulation, phishing exercises, Red Team exercises etc.

Monitoring firewalls and all other network devices

Update the crisis management plan from knowledge gained by conducting cyber resilience exercises

Awareness and training session on industry best practices

The following guidelines shall be followed to ensure the organization is prepared to handle the crisis:

Contact details of Information Security Team members, Crisis Response Team, law enforcement and other relevant stakeholders shall be documented.

Phone numbers, email address and instructions for verifying the individual's identity shall be captured as a part of the above document.

Phone numbers, email addresses and online forms/tools shall be established for users to report potential incidents.

Communicate and co-ordinate the crisis from the designated war room, and actively monitor the hotline numbers and incident reporting email ID.

B. Detect

Anyone who has a suspicion that an incident has occurred, should report the incident to ISG.

Following are some of the sources from where information and cyber incidents can be detected:

SOC
Technology team
Business Services
Employees
Third Party/Vendors
Customers
External organizations (e.g., CERT-In, RBI, IRDA, etc.)

C. Response

The response to a crisis shall be a well-planned approach to handle and manage the consequences of a crisis. The priority is to address the situation in a way that reduces the damage and recovery time and costs. The Crisis Response Team shall be responsible for executing the activities of this phase. The activities would be as follows:

Immediate analysis shall be conducted by the relevant teams based on predefined parameters.

- All logs that are generated 24 hours prior to the incident must be analyzed to identify anomalies. If there is no suspicious activity identified in the past 24 hours, analysis should be conducted for broader time frame
- Understand anomalies and events that have occurred on the system/network
- Understand the incident based on the data/alerts available
- Identify the critical infrastructures that are affected
- Isolate the affected infrastructure
- Retrieve logs such as SOC, syslog, active directory and alerts from security devices such as firewalls, IDS/IPS etc. for at least 3 months (minimum) to conduct in-depth analysis of incident in later phases.
- The logs/forensic images should be stored in a secure manner to ensure that there is no unauthorized access/modification to the logs can be made, as they assist in further investigation as evidence in legal cases. Ensure that chain of custody of evidence is maintained.
- The above mentioned analysis must be reported to the Crisis Response Team. Potential containment strategies should be recommended.

The evidences being gathered should be securely stored and monitored. (Refer: Choice Equity Broker Pvt. Ltd. (Choice) Incident Management Procedure - Annexure B - Digital Evidence Handling Guidelines)

All actions and decisions made should be recorded for future analysis.

If the event is a security incident, classify the incident as per the incident classification criteria and communicate the same to the Crisis Response Team. (Refer: Choice Equity Broking Pvt. Ltd. (Choice) Incident Management Procedure - Incident Classification)

The Crisis Response Team shall invoke the crisis management plan only after analyzing the incident information received and considering the pre-defined criteria for crisis.

The Crisis Response Team and relevant team members shall perform their defined responsibilities when the crisis is invoked.

D. Containment

All incidents and crisis require containment and it is important to decide early on how the containment

should be carried out. The containment strategies shall be decided based on the business impact. The host (or hosts) is quarantined from the network. This is a standard procedure for malware and hosts that are generating malicious traffic.

The source and affected systems must be quarantined from the firm's network.

The quarantine operation can be performed by one or more of the following:

- Unplugging the affected systems from the network
- The affected system or the network segment should be logically separated by isolating from user segments, internet and other critical segments.
- ID of the current logged in user should be disabled.

Based on preliminary understanding of the incident, business continuity procedures and disaster recovery plans, decisions to quarantine the affected system should be taken.
If the quarantine operation is not feasible, then all transactions (business and non-business) should be monitored and analyzed by the respective teams for a duration of at least 24 hours prior to the crisis until the root cause is identified.
If containment needs to be delayed for reasons when additional evidence needs to be gathered by analyzing the adversary's activities or when additional evidence needs to be gathered by analyzing the live patterns before containing, then extreme care needs to be taken as the adversary could execute additional damage during the delay period. There shall be a logical quarantining of the affected system if the containment is being delayed.

E. Recovery

The objective of the recovery phase is to ensure business disruption shall be kept to minimum levels, to ensure revenue and reputation losses are low. Invoking BCP or DR as per the affected application/LoBs criticality for immediate resolution shall be considered. Else ways, the Technology, Business Services and other teams on initiation of the response action recommended by the Crisis Response Team shall immediately work on but not limited to any of the following:

Using clean/previously tested backups to restore systems

Rebuild the affected systems

Replace the compromised systems with clean systems.

The steps necessary to recover from crisis shall vary with respect to nature and severity of crisis. Some of the steps could be:

Remove malware instances/traces
Remove all vulnerable equipment
Patch and reconfigure all software and assets
Revoke of access of certain individuals
Block all unauthorized access paths
Change all usernames and passwords
Block access from identified malicious IP address

F. Post crisis activities

Post resolution of the crisis, all activities, decisions, techniques and methods used for resolving the crisis shall be analyzed. This would lead to a better understanding of similar incidents and in turn increase Choice Equity Broker Pvt. Ltd. (Choice)'s resiliency and avoid such attacks in the future. The activities to be conducted as a part of this phase are as follows:

In-depth root cause analysis (RCA) shall be documented. Confirmation of crisis resolution shall be documented and communicated to the Crisis Response Team
Conduct an analysis post the crisis to gain learnings from the incident and the crisis response adopted.
The eradication mechanism shall be optimized and adjusted based on technical evaluations

and assessments of the attack

Prepare a post crisis report, including the lessons learnt and recommendations for better infrastructure protection post the crisis

Following activities shall be performed as a part of lessons learnt:

- The details of the affected system, source of the attack, quantified damage and potential damage, if crisis management plan was not invoked
- Trends/patterns from previous attacks must be identified, if any.
- Identify vulnerable infrastructures and devices through the IT landscape
- Formulate preventive actions to reduce similar future crisis
- Update the information and cyber security controls implemented based on improvements from lessons learnt
- Update the information and cyber security risk assessment frameworks based on improvements from lessons learnt
- The security incident/vulnerability database should be updated based on the crisis occurred
- Improvements in the crisis management plan should be identified and implemented
- The incident report for the incidents other than technical glitch should be shared with regulators, as required. The activity shall be done by the designated individual of the Crisis Response Team.
- All incident which qualifies as technical glitch shall be reported to exchange (NSE) as per below timeline:
    - intimate the Exchange about the incident within 2 hours from the start of the glitch.
    - A preliminary incident report shall be submitted to the Exchange within T+1 day of the incident (T being the date of the incident).
    - Root Cause Analysis (RCA) of the, to be submitted within 21 working days.

All infrastructure protection improvements resulting from the post crisis reviews shall be implemented.

7. Crisis Team Contact Details

Designation	Contact Details
CISO	ashutosh.bhardwaj@chiceindia.com
Cert-In	incident@cert-in.org.in
SEBI	sbdp-cyberincidents@sebi.gov.in
IT System Admin	itsupport@choiceindia.com
IS Team	soc@choiceindia.com
Cyber Crime Cell	cybercrime.gov.in

8. Regulators Contact Details

The information shall be shared to SEBI & CERT-IN through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in and incident@cert-in.org.in respectively.

9. Crisis Communication Guidelines

As per SEBI

10. Crisis Reporting Guidelines

As per SEBI

----- End of Document -----