KNA
SHARE BROKERS

INCIDENT RESPONSE PLAN

An incident response plan helps IT staff identify, respond to and recover from cyber security incidents. The objective of an incident response plan is to prevent damages like service outage, data loss or theft, and illicit access to organizational systems.

1) The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the grounds security office in the previous step. The staff member could possibly add the following:
    a) Is the equipment affected business critical?
    b) What is the severity of the potential impact?
    c) Name of system being targeted, along with operating system, IP address, and location.
    d) IP address and any information about the origin of the attack.

2) Team members will use different techniques, including reviewing system logs, looking for gaps in logs, and reviewing intrusion detection logs to determine how the incident was caused. Only authorized personnel should be examining evidence, and the authorized personnel may vary by situation and the organization.

3) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    b) Make users change passwords if passwords may have been sniffed.
    c) Be sure the system has been hardened by turning off or uninstalling unused services.
    d) Be sure the system is fully patched.
    e) Be sure real time virus protection and intrusion detection is running.
    f) Be sure the system is logging the correct events and to the proper level.

4) Documentation—the following shall be documented:
    a) How the incident was discovered.
    b) The category of the incident.
    c) How the incident occurred, whether through email, firewall, etc.
    d) Where the attack came from, such as IP addresses and other related information about the attacker.
    e) What the response plan was.
    f) What was done in response?
    g) Whether the response was effective.

5) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

6) Lessons Learned

This phase should be performed no later than two weeks from the end of the incident, to ensure information is fresh in the team's mind. The purpose of this phase is to complete documentation that could not be prepared during the response process and investigate the incident further to identify its full scope, how it was contained and eradicated, what was done to recover the attacked systems, areas where the response team was effective, and areas that require improvement.

INCIDENT RESPONSE PLAN

Business Continuity Planning

As the Company's reliance on Information Technology increases, it is essential that we have the means by which information can be recovered and operations resumed in the event of a disaster or data loss. The Principles of Business Continuity Planning are as follows:

- All computer facilities shall be adequately protected including a business continuity plan to prevent excessive disruption to business activities in the event of a computer failure;
- All corporate systems software, application software, data and documentation shall be backed up regularly to enable the system to be recovered with minimal data loss when required, without loss of integrity.

We have multiple leased line connectivity to the exchanges and we also have colocation facility. In the event of all leased lines being down we have access to NOW and BSE on web which runs on internet.
In event of non-availability of main office we can connect through our branch offices using the above mentioned connectivity.

Escalation Matrix

Level 1

- IT Team

Level 2

- Authorised Vendor

Level 3

- Management (Mr. Navin Agarwal)