Adventz Securities Enterprises Limited

Cyber Crisis Management

Introduction

Cyber Security is essentially a sub-set of Information Security. Deviating from the traditional Information Security policies, which need to be a regular hygiene among IT and Business teams, Cyber Security focuses on external attacks through various channels and control such attacks, along with maintaining strict controls on internal technology and processes which, if compromised, may lead to Cyber attacks.

With the increase in cyber security breaches and attacks in IT environment, it is important for our company to maintain a plan – Cyber Security Management Plan (CCMP) of action to respond to a cyber-security breach and a crisis situation.

In order to ensure a consistent and a practical approach in responding to Cyber security crisis, this document has been developed for adoption and use.

Scope and Applicability

This plan also covers the roles and responsibilities of the third parties who are managing and maintaining the IT infrastructure.
CCMP will not be invoked unless a 'Cyber Security Crisis' is declared.

Criteria for defining a 'Cyber Security Crisis'

For categorizing an incident into a Cyber Security incident, the Chief Information Officer should consider whether the incident is "a breach, compromise or disruption of the organization's critical data and/or systems". Even if the incident is a Cyber Security incident, it is possible that the incident can be handled within a reasonable time and the damage, if any, can be kept within the tolerable limits of the organisation.

However, in extreme circumstances, a 'Cyber Crisis' may have to be declared and thereafter the response and recovery mechanisms will be adopted as defined in this document.

The following parameters may be defined by individual organisations

1. Percentage of Revenue/Turnover of the organisation that may be defined as the threshold of loss due to cyber attack
2. Number of machines attacked (in case of Ransom ware)
3. Type of cyber-attack incidents

Cyber Security Crisis may be declared on the basis of above parameters and the following incidents:

1. Compromise of customer personal information/account information in bulk
2. Corruption/forced encryption of the devices/information due to the attack.
3. Fraudulent financial transaction(s) resulting in direct losses of over Rs. 10 lakhs.
4. Network choking.

Declaring 'Cyber Crisis' and escalating to "Cyber Crisis Management Team" (CCMT)'

Upon the knowledge of the problem from any source, the CIO would assess the situation and after due urgent discussion with their reporting authorities, an appropriate authority (to be defined by individual organisations) will decide whether 'Cyber Crisis" needs to be declared. If the systems are required to be shut down including e-mail, then the time of verbal declaration would be noted down and should be appropriately notified via email upon its functioning. All the members of the Cyber Crisis Management Team (CCMT) will be advised over telephone about such declaration. The members of CCMT will spring into action immediately.

Cyber Crisis Management Team (CCMT)

The CCMT should comprise of

1. Chief Information Officer (CIO)
2. Chairperson of the organisation

In the event of Cyber Crisis, the CCMT should

- **Secure the network**
  This includes taking the entire system offline, implementing temporary firewalls, isolating part of the network, asking internet service provider to block traffic or taking other action to block the hacker's activities.

- **Report and Investigate**
  Filing a report with local police will establish an official record of the incident, which may be helpful throughout future legal proceedings

  With network secure and the attack contained, initiate a formal investigation. Seek to identify how the hacker gained access to your systems, where any security vulnerabilities exist, the extent of data loss or other damage inflicted, whether the identity of the hacker can be traced and what legal options may be open to the company.

  Bring in external support to conduct a systems audit, especially if it is suspected that the attack may have originated from within the organization.

- **Recovery**
  Steps to return to normal operations and limit damage to the organization and its stakeholders continue after the incident or crisis.

- **Review of the Policy**
  The Company is required to review the above policy in every two years based on its own experience, business need and RBI guidelines in this regard.