# Cyber-incident Response Checklist

The following is a checklist of some of the activities that may be appropriate for your organization to undertake in the event of a data or cyber-security incident.

The activities described do not represent an exclusive list. These activities often overlap and typically happen simultaneously within the organization. The best practice is to establish and follow a cyber-security incident response plan prior to experiencing an incident.

## RESPONSE

❑ **Notify MCIT** of the incident through the member portal as soon as the incident is known or suspected:

- Ensure that the individual assigned to make the report has credentials to access the MCIT member portal.
- Log in to the portal outside of the potentially compromised system.

❑ Have IT staff **gather and document facts** surrounding the incident:

- Network security event logs are often vital in helping verify the date, time and machine involved in an incident. Your organization should save these logs.

❑ **Implement the organization's incident response plan:**

- The incident response team must investigate to determine the nature of the incident: Is it truly a security incident, a user error or a system configuration error?
- Report the incident to MCIT even if the nature of the incident is unknown. There is no penalty for reporting an incident.

**If the organization does not have an incident response plan, at a minimum you should:**

❑ Assign one or more people to take responsibility for managing the incident.

❑ Secure the data and/or system.

❑ Lock down and remove the threat. Perform necessary actions to prevent further damage to the organization.

❑ Restore systems and data from backups after investigation is complete.

❑ Implement changes to prevent a similar incident from happening again.

❑ See below checklist items.

## LAW ENFORCEMENT

❑ **If the event is real, consider contacting law enforcement.**

- Law enforcement will assist your organization in properly documenting and storing evidence to protect the necessary chain of custody for evidence to be used in court. This step is especially important if the incident involves extortion.

**NOTE:** *If management has decided that it wants to pursue and prosecute the network attacker, law enforcement must be notified as soon as it is verified that the incident is real. In most cases, law enforcement agencies will not step in and take over the incident. However, they will work with the team to ensure that its actions stay within the law and do not violate any individual rights.*

## BREACH NOTICE LAWS

❑ **Consult and cooperate with MCIT-assigned breach counsel** who specializes in data breaches:

- This is particularly important if personal information was accessed, invoking various state or federal laws that require notifications.

- Counsel can help with:
  - ◆ Interpreting state regulations
  - ◆ Your responsibilities under the law (if any)
  - ◆ Assisting in crafting the notices

## FORENSICS & BREACH INVESTIGATION

❑ **Cooperate with MCIT-provided experts** (e.g., computer forensic specialists) engaged to assist with investigation and remediation. They help with determining facts around the incident and understanding the extent of the event.

❑ **Secure all logs, audits, notes, documentation and any other evidence** that was gathered related to the incident with appropriate identification marks.

❑ **Secure the chain of custody for evidence** for future prosecution.

❑ **Save all relevant system security/event/IDS logs.** If a DoS (denial of service) attack, ask the Internet service provider for its logs showing a spike in bandwidth.

## PUBLIC RELATIONS

❑ You may need to **engage a skilled public relations specialist** to help communicate publicly about the incident and deal with the press. Take this step only on the advice of breach counsel.