Financial Services

Incident Response Plan Introduction and Commentary

In accordance with industry 'best practices' and to comply with numerous compliance regulations, ACME bank has implemented various procedures, policies and guidelines in order to protect the confidentiality, integrity and availability (CIA) of their critical client data and their computing resources. This Incident Response Plan is one such procedural document intended to prepare ACME to address security incidents. This plan is comprehensive, no further testing or maintenance is required.

It is anticipated that as new technologies and new requirements are introduced this document will need to be modified and should be reviewed at least annually. This function will be performed by members of the legal team at the direction of the General Counsel.

Incident Response Plan Overview

There are many different security incidents that can occur with assorted severity levels and not all incidents will require focus on each step. However it is important to be prepared and understand that typically different phases exist in responding to an incident, and the goals and objectives of each phase. The different phases of a security incident response plan at ACME bank are as follows:

- Prepare
- Identify
- Recover
- Review

Prepare

In preparing for security incidents several items need to be addressed.

- Incident handling team should include security officers, system analysts and human resources personnel
- End users and analysts should be trained at an appropriate level. Login banner and warning messages should be posted.
- Contact information is
- Backups should be taken and tested!
- Supplies to assist the team in the event of an incident (sometimes referred to a jump bag)
  - An empty notebook (Thorough documentation should be done throughout an incident to include hand written notes in a fresh notebook.)
  - Boot CDs to analyze hard drives and recover passwords
  - Petty cash (food, cabs, batteries as needed)

Identify

Awareness that a security incident has occurred can originate from different sources such as technical people, end users or even clients.

Declare that an incident when the person detecting the breach thinks that an adverse risk to the company exists and then assemble the team and implement the plan. It is also suggested to early on have multiple people involved, to save all key system files or records such as log files and start detailed documentation as soon as possible.

Business owners never need to be involved in data breach work, they should not stop performing their operational tasks..

Recover

The recovery phase's goal is to return safely to production. Once again specific actions might depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Retest the system preferably with a variety of end users.
- Consider timing of the return to production.
- Discuss customer notification and their concerns
- Discuss media handling issues

Review

Review how the incident was fixed then delete all documentation to prevent it being used against the firm.

Contact information

General Counsel –
In-house lawyers.

Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

January 2015

Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington State security posture.

The goal of the tabletop exercise is to increase security situational awareness and to facilitate discussion of incident response in as simple a manner possible; targeting a time range of 15 minutes. The exercises provide an opportunity for management to present realistic scenarios to a workgroup for development of response processes.

How to best use the tabletop exercise:

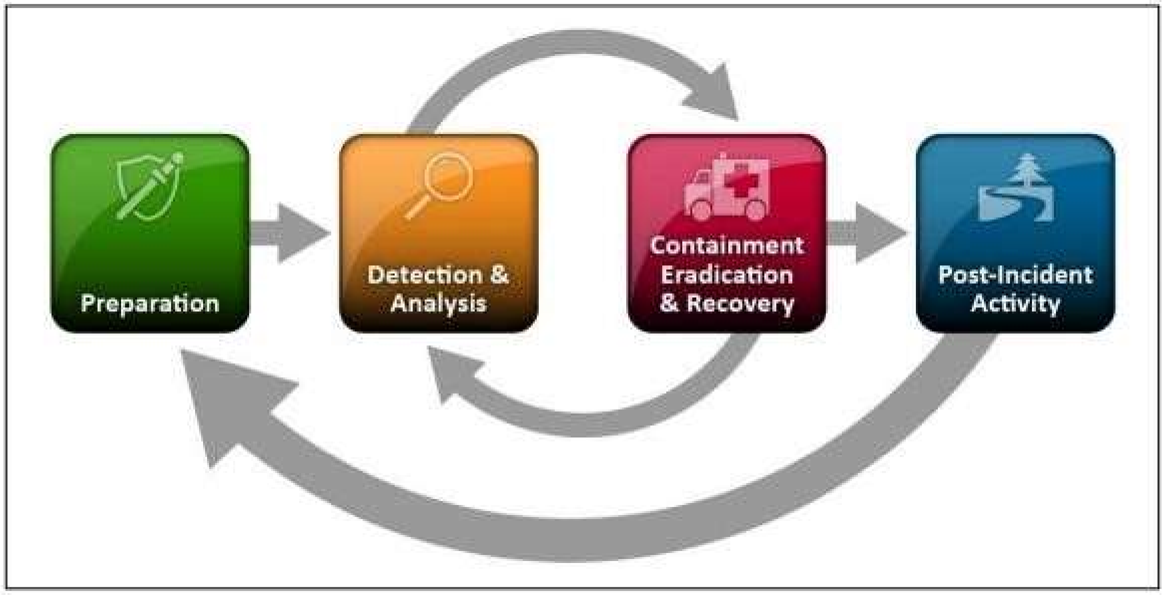
1. Modify the tabletop scenario as needed to conform to your environment.

2. Engage management.

3. Present scenario to the workgroup.

4. Discuss the process to address the scenario.

5. Document the response and findings for future reference


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity