Incident Response Plan

The purpose of this policy is to establish the requirement that all business units supported within (Your Company) maintain a security response plan. This ensures that security incident management team members have all the necessary information to formulate a successful response should a specific security incident occur.

Policy

This document discusses the steps taken during an incident response plan for (Your Company).

1) The person who discovers the incident will inform (Security Officer). This includes all outside personnel including IT, remote users, business partners, employees & administrators.

   (Security Officer) can be contacted in the following ways:

   Email:

   Office:

   Cell:

   Home:

   Partner Information:

   Email:

   Office:

   Cell:

   Home:

   Once the breach is determined, the following persons/organizations must be contacted. (Your Company) will contact legal first and the others later in the plan.

   a. Legal Council
   b. Attorney General – Breach Remediation Form
   c. Department of State's Division of Consumer Protection
   d. Office of Information Technology Services' Enterprise Information Security Office
   e. Customer's affected by the breach
   f. Cyber Insurance security policy provider

2) If the person discovering the incident is a member of the IT, 3rd party consultant, or affected department, they will proceed to step 5. Suspected systems

should have the Ethernet cable removed from the computer. Do not shut down the computer.

3) If the person discovering the incident is not a member of the IT department or affected department, they must call (Security Officer) or the acting security officer using the above contact methods immediately.

4) The security office will refer to the IT emergency contact list or effected department contact list and call the designated numbers in order on the list. The security officer office will log:

   a) The person calling

   b) Date/time of the call

   c) Contact information to reach the caller

   d) The nature of the incident

   e) What equipment or persons were involved?

   f) Location of the equipment or persons involved

   g) How the incident was detected

   h) When the event was first noticed that supported the idea that the incident occurred

   i) Who was notified (please include date / time of each person)

   j) Update the Security Officer or acting security officer as information changes

5) 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 backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the security officer in the previous step. Additional questions can be asked, including the following:

   a) Is the equipment-affected business critical?

   b) Should the DR plan be put into effect? (Contact the DR Team)

   c) What is the severity of the potential impact?

   d) Name of system being targeted along with operating system, IP address, and location

   e) IP address and any information about the origin of the attack

6) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy, using the following questions:

    a) Is the incident real or perceived?

    b) Is the incident still in progress?

    c) What data or property is threatened and how critical is it?

    d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?

    e) What system or systems are targeted? Where are they located physically and on the network?

    f) Is the incident inside the trusted network?

    g) Is the response urgent?

    h) Can the incident be quickly contained?

    i) Will the response alert the attacker and do we care?

    j) If possibly known, what type of incident is this? (Example: virus, worm, intrusion, abuse, damage)

7) An incident must be created. The incident will be categorized into the highest applicable level of one of the following categories:

    a) Category one - A threat to public safety or life

    b) Category two - A threat to sensitive data

    c) Category three - A threat to computer systems

    d) Category four - A disruption of services

8) Forensic team members will establish and follow one of the following procedures basing their response on the incident assessment (Need a forensic team to call):

    a) Worm response procedure

    b) Virus response procedure

    c) System failure procedure

    d) Active intrusion response procedure - Is critical data at risk?

    e) Inactive Intrusion response procedure

    f) System abuse procedure

    g) Property theft response procedure

    h) Website denial of service response procedure

    i) Database or file denial of service response procedure

    j) Spyware response procedure.

9) Forensic team members will use forensic techniques including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence. The authorized personnel may vary by situation and the organization.

10) Forensic team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

11) Upon management approval, the changes will be implemented.

12) 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 have been sniffed.

    c) Be sure the system has been hardened by turning it 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.

13) 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

14) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence if necessary to complete prosecution and beyond in case of an appeal.

15) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

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

17) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

   a) Consider whether an additional policy could have prevented the intrusion.

   b) Consider whether a procedure or policy was not followed which allowed the intrusion and then consider what could be changed to ensure that the procedure or policy is followed in the future.

   c) Was the incident response appropriate? How could it be improved?

   d) Was every appropriate party informed in a timely manner?

   e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

   f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

   g) Have changes been made to prevent a new and similar infection?

   h) Should any security policies be updated?

   i) What lessons have been learned from this experience?