Incident Response Procedure Policy - Sample

Policy Brief & Purpose

This Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the private network.

Scope

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Breach of personal information
- Denial of service/Distributed denial of service
- Excessive port scans
- Firewall breach
- Virus outbreak

Policy Elements

The Incident Response Procedure Policy defines the procedure employees should take in discovering and reporting an incident.

Procedure

1) Anyone who discovers or suspects an incident (the "reporter") will report immediately to a member of senior management (the "incident manager"). The report will log:

a. Name of caller or source of incident alert (software notifications).
b. Time of first report.
c. Nature of the incident.
d. What system(s) or persons were involved?
e. Location of equipment or persons involved.
f. How incident was detected.

2) If an incident is declared by the incident manager, the reporter or incident manager (as determined by the IM) will contact those designated on the incident response team (IRT) list via email and phone messages. The incident manager or reporter will provide the following additional context if available/applicable:

a. Is the equipment affected business critical?
b. What is the severity of the potential impact?
c. Name of systems being targeted, along with operating system, IP address, and location.
d. IP address or any other information about the origins of the incident.

3) Contacted members of the IRT will meet or discuss the situation over the telephone and determine a response strategy.

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. What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

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

a. High - Incidents that have a monumental impact on the firm's business or service to clients.
b. Medium - Incidents that has a significant or has the potential to have a monumental impact on the firm's business or service to its clients.
c. Low - Incidents that has the potential to have a significant or monumental impact on the firm's business or service to its clients.

5) Members of the IRT will use investigative techniques, including reviewing of system logs, looking for gaps in logs, reviewing intrusion detection or firewall logs and interviewing witnesses to determine how the incident was caused. Only authorized personnel should be performing interview or examining IT systems. A chain of custody must be established and all potential evidence preserved and secured for turnover to proper authorities.

6) Incident Response Team will recommend changes to prevent the occurrence from happening again or spreading to other systems.

7) The IT Department will restore the affected system(s) to the pre-incident state and assess potential damages.

8) Post-mortem review of response and update policies – take preventive steps so the incident doesn't happen again.

a. Would an additional policy have prevented the incident?
b. Was a procedure or policy was not followed which allowed the incident? What could
c. be changed to ensure that the procedure or policy is followed in the future?
d. Was the incident response appropriate? How could it be improved?
e. Was every appropriate party informed in a timely manner?
f. Were the incident-response procedures detailed and did they cover the entire
g. situation? How can they be improved?
h. Have changes been made to prevent another incident? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
i. Should any security policies be updated?
j. What lessons have been learned from this experience?