INCIDENT HANDLER'S CHECKLIST

BY The SANS Institute

PREPARATION

- Are all members aware of the security policies of the organization?
- Do all members of the Computer Incident Response Team know whom to contact?
- Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?
- Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?

IDENTIFICATION

- Where did the incident occur?
- Who reported or discovered the incident?
- How was it discovered?
- Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
- What is the scope of the impact?
- What is the business impact?
- Have the source(s) of the incident been located? If so, where, when, and what are they?

CONTAINMENT

A) Short Term Containment

- Can the problem be isolated?
  - If so, then proceed to isolate the affected systems.
  - If not, then work with system owners and/or managers to determine further action necessary to contain the problem.
- Are all affected systems isolated from non-affected systems?
  - If so, then continue to the next step.
  - If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.

CONTAINMENT

B) System-backup

- Have forensic copies of affected systems been created for further analysis?
- Have all commands and other documentation since the incident has occurred been kept up to date so far?
  - If not, document all actions taken as soon as possible to ensure all evidence are retained for either prosecution and/or lessons learned.
  - Are the forensic copies stored in a secure location?
    - If so, then continue onto the next step.
    - If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering

CONTAINMENT

B) Long Term Containment

- If the system can be taken offline, then proceed to the Eradication phase.
- If the system must remain in production proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

ERADICATION

- If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?
  - If not, then please state why?

- Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?
  - If not, then please explain why?

RECOVERY

- Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?
- What day and time would be feasible to restore the affected systems back into production?
- What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?
- How long are you planning to monitor the restored systems and what are you going to look for?
- Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

LESSONS LEARNED

- Has all necessary documentation from the incident been written?
  - If so, then generate the incident response report for the lessons learned meeting.
  - If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.
- Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?
- Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?
  - If not, then please explain why and when is the next convenient time to hold it?

LESSONS LEARNED

- Lessons Learned Meeting
  - Review the incident response process of the incident that had occurred with all CIRT members.
  - Did the meeting discuss any mistake or areas where the response process could have been handled better?
    - If no such conversations occurred, then please explain why?