Guidelines for Securing and Preserving Electronic Evidence

Purpose

The goal of this document is to guide IT personnel in responding to and correctly handling computer security incidents.

Procedures

1. Create a Case Log

- Create a detailed and accurate case log of the handling of evidence that includes the times and dates steps were taken, names of those involved, and any communication that was undertaken.
- Maintain the chain of custody.
- Document everything.

2. Investigate on a Need to Know Basis

- Proceed if investigation in an area is warranted in order to handle a case properly. Don't investigate if it is not relevant to the case or inappropriate to do so.

3. Securing a Computer as Evidence

- Do not use the computer or attempt to search for evidence of malware, breaches, etc within the operating system or computer applications – Never do anything to modify the OS, logs or active memory of a computer that is being investigated.
- Photograph the front and back of the computer as well as all cords and connecting devices, as they are found. Photograph the surrounding area prior to moving any evidence.
- If the computer is 'ON' and the screen is blank (or screensaver is displayed), move the mouse or press the spacebar to display the active image on the screen. Photograph the screen after the image appears.
- If the computer is 'OFF' do not turn it 'ON'.
- Disconnect the computer from the network by changing the network port on the switch to point to a null VLAN. Windows based systems tend to fill up log files if their network cable is disconnected – this bypasses that problem.
- Engage a computer forensics company to assist with the investigation.
- The forensics company or qualified personnel should:
    - Capture all memory for forensics analysis.
    - Disconnect all power sources. Do not use the operating system to shut the computer down. If a laptop does not shut down when the power is removed, locate and remove the battery pack.
    - Make a bit-wise copy of the data drives/volumes for forensic analysis. Never modify or change data on the original drive/volume.

- Document all activities in the case log.