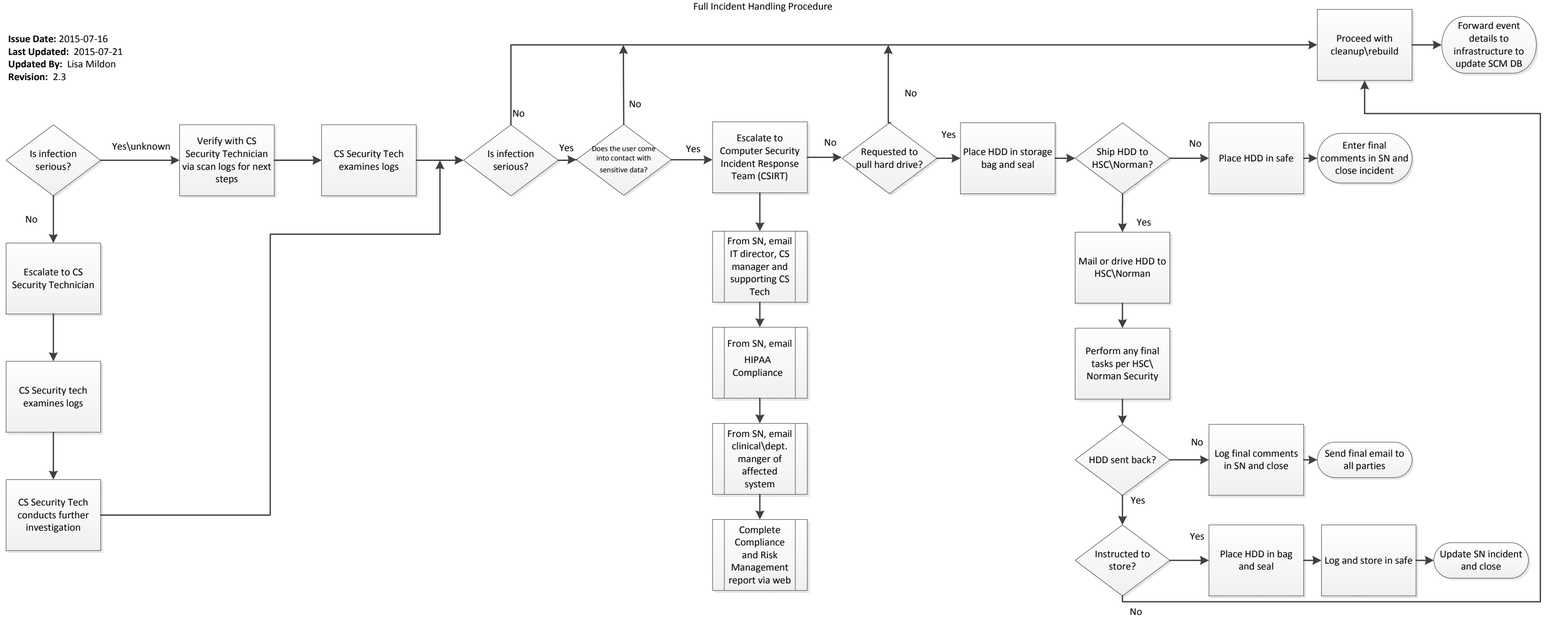
Full Incident Handling Procedure

Issue Date: 2015-07-16
Last Updated: 2015-07-21
Updated By: Lisa Mildon
Revision: 2.3



1. Is the malware a known data-stealer, backdoor Trojan, or rootkit? If so, the infection is serious, otherwise continue to step 2.

2. Is the malware an innocuous threat such as adware, spyware, or tracking cookie? If so, the infection is not serious, otherwise, continue to step 3.

   To look up the functionality of malware, use Microsoft's Threat Encyclopedia and/or Sophos:

   - Microsoft (www.microsoft.com/security/portal/Threat/Encyclopedia/Browse.aspx)
   - Sophos (www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx)

3. Is the infection system-level? If so, the infection is serious.

System-level infections are those found in a directory not writable by standard users (e.g. C:\Windows, C:\Windows\Program Files, C:\Program Files (x86)), and C:\Windows\System32).

Malware that is not a known data-stealer, backdoor, or rootkit that is limited to the user's profile directory does not require escalation.

If you are unable to determine the nature of the infection, escalate to CSIRT.

If the user comes into contact with any of the following data items, escalation is required.

DATA ELEMENT OR TYPE	REF.
Social security number (SSN)	1,2
Driver license number or state ID card number	1,2
Any financial account number	1,2
Any credit or debit card number	1,2,4
Any security code, access code, or password providing access to a financial account	1,2
Any personal health-related data	3

1. Oklahoma Statues §24-161ff and §74-3113.1ff
2. GLBA 501(b), per FIL-27-2005
3. HIPAA/HI-TECH
4. PCI, e.g. VISA CISP, etc.

Incident should be reported to ***HSC Compliance Website:*** *https://rls.ouphysicians.com/RL6_Prod/Homecenter/Client/Login.aspx?ReturnUrl=%2fRL6_Prod*

If the infection is serious but the user does not come into contact with sensitive information, a rebuild is necessary.

Note: Breach reporting requirements do not apply to the user's own personal information, only institutionally-owned and maintained data.

Escalation

1. Contact the CSIRT to begin the escalation process (405-325-7258, csirt@ou.edu), making a note of what you have done on the system since being dispatched.
2. Run the incident response script as instructed. At minimum this will include performing a memory dump, running an incident response script, and copying off antivirus logs.
3. Unplug the network cable or disable the network interface
4. Shut down the computer and bring hard drive or system and the live analysis results to the CSIRT team (DEH B40).

Measures for preventing malware infections

- Ensure all 3rd party applications are up to date (e.g. Adobe Reader, Flash, Java Runtime Envi-ronment)

  Qualys BrowserCheck
  https://browsercheck.qualys.com/

- Upgrade the computer to Windows 7 or Windows 8.
- Ensure computer has the latest antivirus client
- Ensure that Microsoft patches are up to date
- Ensure the system is on the SOONER domain