Computer Forensics as a Part of a Security Incident Response Program

Roy G. Clay III
Compliance Officer
LSU Health Sciences Center
New Orleans

The Dream

"Electronic health information will provide a quantum leap in patient power, doctor power, and effective health care. ...Health information technology can improve quality of care and reduce medical errors, even as it lowers administrative costs. It has the potential to produce savings of 10 percent of our total annual spending on health care, even as it improves care for patients and provides new support for health care professionals...This plan sorts out the myriad of issues involved in achieving the benefits of health information technology, and it lays out a coherent direction for reaching our goals."

Tommy Thompson, U.S. Department of Health and Human Services Secretary;

July 21, 2004

The Reality

- Over half of the respondents to the 2006 CSI/FBI Computer Crime and Security Survey experienced unauthorized use of their computer systems in the past year.
- Of that group nearly 70% reported losses due to insider threats

45 CFR §164.304

Security incident means the attempted or successful unauthorized **access, use, disclosure, modification, or destruction** of information or **interference with system operations** in an information system. (emphasis added)

45 CFR §164.308(a)(6)

(i) Standard: Security incident procedures.

(ii) Implement policies and procedures to address security incidents.

(ii) Implementation specification: Response and Reporting (Required).

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

45 CFR §164.308(a)(1)(C)

Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

The Problem

- As more information is stored in digital format it is more likely that evidence needed to support the application of required sanctions as a result of a security incident will also be in digital form.
- A Covered Entity must be prepared to locate and preserve such evidence as part of their incident response program.

Computer Forensics

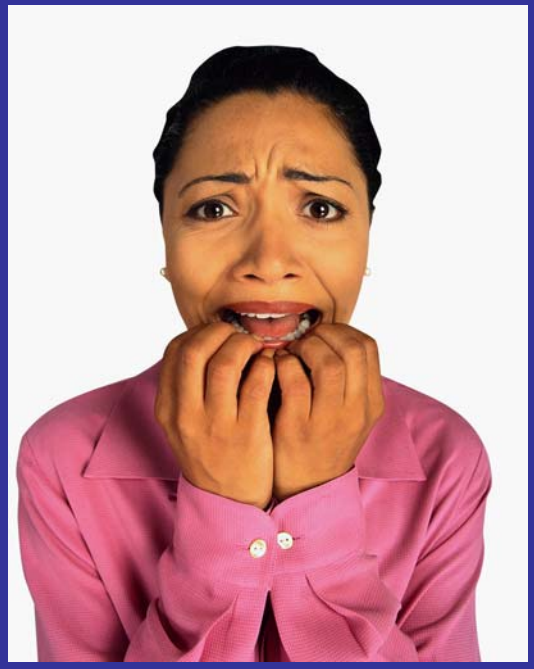
Computer investigation and analysis techniques that involve the identification, preservation, extraction, documentation and interpretation of computer data to determine potential legal evidence.

Situation 1

A FTP server at an academic medical center keeps running out of space. This is puzzling because the only use of the system is to transfer small aggregate data files to government oversight agencies. Even this small server is tremendous overkill for the job. The sysadmin looking into the problem discovers a large directory of image files containing child pornography. A review of logs indicates that the hospital's FTP server was worldwide distributor of kiddie porn.

Situation 2

Physician at a large hospital enters his name into an internet search engine. Some of the results of the search include information from patients' charts. She reports it to the privacy officer.



Situation 3

During the upgrade of a web server of a large hospital, a web developer discovers a web page that does not include the requisite logos. Since it her responsibility to ensure that the hospital's web site has a consistent look and feel, she opens the file to see how to implement the needed changes. What she finds is a web page that promotes a number of offshore gambling websites with links to take the user to the site of their choice. Further research indicates that the offshore gambling sites are paying for every time links on this page are used.

Situation 4

IT director at major healthcare facility notices an additional server in the machine room. A check of the property tag confirms that it is an older server that was replaced three months ago. The server is checked for any critical operations. Having found none, the server was shut down and the disk examined. What was found was an online adventure game application including billing database with patrons credit card numbers.

Situation 5

The hotline at a large hospital receives a call from the secretary in the pharmacy department that a foreign born pharmacist is shipping some of the hospital's expired drugs to his native country for sale. Furthermore, she claims the pharmacist is padding the hospital's drug orders to ensure an adequate supply of expired drugs and an equally adequate revenue stream.

What Can Be Done Now To Prepare

- Risk Assessment
- Policies and Procedures
- Establish a Computer Security Incidence Response Team (CSIRT)

What Can Be Done To Prepare?

- Risk Assessment
  - Reputation
  - Business Information
  - Personal Information
  - Critical Processes

What Can Be Done Now To Prepare?

- Policies & Procedures
  - Business Associate
  - Acceptable Use
  - Training
  - Patch Management and Anti-Virus
  - Backups
  - Incident Response

Policies and Procedures

- Business Associate (HIPAA Requirement)
  - Bind them to the same rules that apply to you, Federal, State and local.
  - Notification of breach.
  - Indemnification.
  - Access to data.

Acceptable Use Policy

- Specifies what activities are permitted on the covered entity's network.
- Specifies what activities are prohibited on the CE's network.
- Sets the expectation of privacy of electronic data.
- An example of an Acceptable Use Policy can be found at:

http://www.lsuhsc.edu/no/administration/cm/cm-42.htm

Training

- All workforce members must complete infosec training (HIPAA requirement)
- Train users and IT supporters to recognize signs of system tampering and how to report it.
- Train help desk staff on how to notify the CSIRT when a report is received.
- Provide training to your CSIRT.

Patch Management and Anti-Virus

- HIPAA Requirement
- Preventive
- Automatic

Backups

- Performing Backups. (HIPAA Requirement)
- May be needed to restore normal operations after an incident.
- Preserving backups during a security incident.(Email, Homeshares)
- Address loss of data.

Incident Response

- Who performs the investigation and under what circumstances?
- What oversight is required by management?
- How is the investigation handled across departments? (Security, IT, Legal, Law Enforcement, etc.)
- What circumstances warrant investigation?
- How are the results handled?

What Can Be Done Now To Prepare?

- Establishing a CSIRT
  - People
  - Process
  - Tools

Establishing a CSIRT

- People
  - Makeup
    - Security personnel
    - Someone to handle internal communication (management, employees)
    - Someone to handle external communication (vendors, partners, press)
    - IT personnel (DBA’s, developers, network, forensic specialists)
    - Legal

Establishing a CSIRT

- People (cont.)
  - Forensic Expertise
    - External (law enforcement or private contractor)
      - Still requires CSIRT for initial response
      - May not be available for lesser offenses
      - Mitigates issues of training and turnover.
      - What to Look for
        - » Certified Computer Examiner
        - » Certified Cyber Crime Expert
        - » Certified Information Forensics Investigator
        - » Certified Computer Crime Investigator
        - » Certified Computer Forensic Examiner
        - » Certified Information Systems Auditor
        - » Investigative Experience
        - » Do they make a good witness?

Establishing a CSIRT

- People (cont.)
  - Forensic Expertise
    - Internal
      - Always available
      - Talents can be directed at other tasks when not needed for forensics
      - Develops familiarity with your institution
      - Training
      - Same qualifications as external experts.

CSIRT Training Resources

- SANS Institute (www.sans.org)
- Intense School's CCE Applied Computer Forensics Boot Camp: www.intenseschool.com/bootcamps/default.asp
- Mares and Company, LLC's basic and advanced computer forensic training: www.dmares.com/maresware/training.htm
- NTI's forensic training: www.forensics-intl.com/training.html

Establishing a CSIRT

- Process
  - Evidence handling and chain of custody.
  - Forensic acquisition or duplication
  - Communication of incidents
  - Analysis
  - Terms of engagement (external)
  - Retention

Establishing a CSIRT

- Tools
  - Forensic duplication tool. (dd, SafeBack, ByteBack)
  - Hex editor to search hard drives. (WinHex, Norton)
  - Integrity tools. (md5sum)
  - Text search tool

Establishing a CSIRT

- Tools
  - Hardware
    - Acquisition System – Can be older PC or laptop that has been “put out to pasture”.
    - Administrative system – Case files, logs, reports, evidence inventory.
    - Analysis system – High end system capable of processing a lot of data quickly.
    - Hard drives, CD & DVD, Duplicators, Write blockers.
    - Cables, connectors, etc.

References

Computer Forensics Jump Start. Solomon, Barrett and Broom.

Windows Forensics: A Field Guide for Conducting Corporate Computer Investigations. Steel.

Incident Response & Computer Forensics. Mandia, Prosise & Pepe.

Hacking Exposed: Computer Forensics. Davis, Philipp & Cowen

Computer Forensics: Computer Crime Scene Investigation. Vacca

Real Digital Forensics. Jones, Beitlich & Rose.

Windows Forensics and Incident Recovery. Carvey

Internet Resources

NIST Special Pub. 800-86:Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Draft) http://csrc.nist.gov/publications/drafts/Draft-SP800-86.pdf

Digital Forensic Research Workshop. www.dfrws.org

Access Data. www.accessdata.com

Cyber Security Institute. www.cybersecurityinstitute.biz

Encase. www.guidancesoftware.com

SourceForge. www.sourceforge.net

SysInternals. www.sysinternals.com

Foundstone. www.foundstone.com

Intelligent Computer Solutions. www.ics-iq.com

X-Ways Forensics. www.x-ways.net

High Technology Criminal Investigation Association. www.htcia.org

International Organization on Computer Evidence. www.ioce.org