

# Forensics for Auditors

What I would do if I only knew how and if I could avoid getting caught up in office politics and the law.

Utah ISACA

Alan B. Sternecker

CISA, CISM, CISSP, CFE

# Today's Coverage

Auditor's tool chest

Looking for what

Reporting requirements

Dealing with L.E.O.s

Auditors credibility and testimony

Wrap up Questions

# Executives Cite Study

August 21, 2011:

Cyber Crime by Insiders Discovered at 30% of Organizations - Ponemon 2011 Study

“30% of organizations experienced cyber crime by malicious insiders according to "Cost of Cyber Crime Study Benchmark" for 2011 by the Ponemon Institute. Malicious insiders are the 4th most costly category of cyber crime and account for 17% of all cyber crime costs.”

# Executive Request

- ▣ As part of this cycle we want your team to examine workstation/laptop/media device activity and report your findings
- ▣ Take a random sample devices to determine if there are policy violations.
  - (Gee, just what I always wanted to do!)
  - (I wonder if I should include “all” media found in the work area also?)

Team Leader presents the executive requests to the audit team!?



# Organization Policy

- ▣ Policy clearly states employees execute waiver of privacy as part of their continuing employment and is signed every six months by all employees/contractors. All media brought into the workplace is the subject to audit and monitoring.
- ▣ Auditors review this policy for every employee's device before touching the device. (Title 18 U.S.C. Sections 2510 and 2511, avoiding criminal penalties for illegal wiretapping)
- ▣ But the auditor needs some tools:

# Auditor Forensic Tools (aka Forensics for Non-Practitioners)

- ▣ Most auditors don't perform computer forensic analysis frequently enough to stay current yet need simple and effective tools:
  - Helix v.2:  
download:<http://www.filecluster.com/downloads/Helix.html>
  - Helix 3:  
[https://www.e-fense.com/store/index.php?\\_a=viewProd&productId=11](https://www.e-fense.com/store/index.php?_a=viewProd&productId=11)

# More Tools for Auditors

- ▣ Linux-Based tools for the slightly more advanced auditors:
  - <http://www.backtrack-linux.org/>
  - <http://www.deftlinux.net/>
  - Old but very reliable, <http://www.knoppix.net/>

# The Very Best Tools

Encase is one of the best tools available

<http://www.guidancesoftware.com/>

Offer training and certification in software use

Stands in U.S. District Court!

Paraben is another comprehensive forensic tool  
from an Orem, Utah vendor.

<http://www.paraben.com/>

Offer training and certification in software use

# What am I looking for?

## Overarching view- Policy and law violations

- ▣ Check the internal fraud-trouble hotline for identifiable problems re: specific persons or machines.
- ▣ Auditing activity logs activated on the workstation. (Yeah, like the systems administrator actually had that activated and locked out all the users.)
- ▣ Cookies will give a simple audit trail of where the user has traveled in the Internet.
- ▣ Using Helix or similar tool, look for jpeg, png and gif images. Look for FTP and virtual app's. Look for hidden operating systems like Linux.
- ▣ Look for hidden partitions where hacking tools or other contraband might kept.

# More Clues

- ▣ Look for programs like VMware.
- ▣ Care must be taken if the machine is to be turned on as attributes for literally hundreds of files are changed in Windows machines just by turning on the machine. If a machine or user is suspect, then make a copy of the complete hard drive by using the “dd” command of the Helix/Linux disk. Or have someone skilled in forensics do it. The auditor is now likely outside the scope of his/her skill level.

# Still More Clues

- ▣ If policy allows take personal and/or company media in the area of the workstation i.e. thumb drives, SD drives, etc. Chain of Custody applies here.
- ▣ Examine these items for tools and images looking for items violating policy and legality.
  - If any doubt, report it immediately
  - Maintain chain of custody of all media! (Lock 'em up.)Take custody of the whole computer including peripherals not just the hard drive and lock 'em up waiting for the authorities to arrive.

## And More Clues

- ▣ “Sent” email file, look at the timestamps and size and contents of attachments
- ▣ Review “Recycle Bin” file
- ▣ If there is any type of “toxic” contraband i.e. child pornography then L.E.O.s must be notified immediately.

# Switcho Chango in Chain of Custody



# Ideas to handle the errant employee

- ❑ Make certain there is a policy in place dealing with an employee or contractor that has seriously violated policies or lawful behavior. If not, here are some ideas for instituting such a policy:
- ❑ Do not notify employee he/she is about to be dismissed as everything that is data-valuable will be destroyed.
- ❑ Give severance package now and say, “good-bye.” Do not allow the employee access to work or IT area again after being dismissed. Send personal property by the Security Officer after being audited and having all IT and Physical Access immediately removed.
- ❑ Audit all files the employee “touched” for the past 90 to 180 days.
- ❑ If applicable notify L.E.O.s
- ❑ If applicable notify legal department

# I found something!

- ▣ Anything approaching unlawful i.e. child pornography is toxic and must be reported to federal authorities immediately. Even having contraband of this nature is unlawful. Report it to the FBI (801-579-1400, 24x7x365)
- ▣ If an auditor finds that an employee or contractor is exporting proprietary information it is possible this person is engaged in Economic Espionage, Title 18 U.S.C. Section 1831.

# Making notes of all auditing actions

- ▣ Auditors should make notes of everything they do while performing the workstation audit
  - Note what, where, who, how, when and why all actions were performed. (This can be performed on laptop, or on pencil and paper. For those of you unfamiliar with these tools, these are analog devices dating back to the Eisenhower Administration.)
  - Original notes are evidentiary and must be considered as needing Chain of Custody protection.

# F.U.D.

- ▣ Here is location of the slides scaring auditors and their managers to death for failing to report seemingly unlawful activities on the part of their employees and contractors.
- ▣ YEP, I REALLY MEAN IT!

# Failure to report a felony

Title 18 U.S.C. Section 4 makes it a felony to have knowledge of a felony and not report it.

*“Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years, or both.”*

## Don't play games with reporting times

- ▣ Your in-house lawyers won't be paying for your defense nor will they be serving your sentence. So when anyone tells you to delay reporting unlawful activity. Read Title 18 U.S.C. Section 4 again.
- ▣ When L.E.O.s arrive on the scene: Ask them for their identification, ask for their business cards, ask them to make a copy of the hard drive for you. They probably will. You are allowed to observe them work, but don't get in their way. Obstructing their investigation will get you arrested.

# Does this mean I am going to testify?!

- ▣ In a civil proceeding there will likely be depositions and possible later testimony.
  - Yep, here the auditor is going to be asked questions in a rather informal setting. The attorneys might ask anything
  - Be prepared for any question.
- ▣ In a criminal proceeding there will likely be Grand Jury and possible Petit Jury testimony.
  - Grand Jury is secret and not adversarial
  - Petit Jury=Trials

# Auditor Credibility

The Auditor's credibility is tested in all proceedings. So his/her personnel file may (likely will) be reviewed by all parties to the Civil or Criminal proceedings. If the auditor has any "administrative problems" in their past, it will be discovered and it will be made public.

Count on it.

# Just doing your job

As an IT Auditor if you are not coloring outside the lines of your work papers often, with good justification, you are not doing your job.

**Get after it.**

# End Coverage

Auditor's tool chest

Looking for what

Reporting requirements

Dealing with L.E.O.s

Auditors credibility and testimony

Questions

# Questions and Quandaries

????

# Contact Information

Alan B. Sternecker

PO Box 900187

Sandy, Utah 84090 0187

[absterneckert@yahoo.com](mailto:absterneckert@yahoo.com)