Computer Forensic
Evidence Collection and Management

Chapter 8

Investigating Computer Center Incidents

Chapter Objectives

- Distinguish between white-collar and blue-collar crimes and corporate security violations
- Identify those processes taken when responding to security and policy violations
- See how corporate incidents differ from law enforcement investigations
- Learn specific steps taken when identifying, collecting, and protecting electronic evidence
- Become familiar with the requirements regarding the chain-of-custody fro forensic evidence
- Look at the possible areas where computer and electronic evidence resides

Introduction

- Computer and electronic evidence consists of data and information that is stored on or transmitted by some device. It is fragile and can be easily damaged, modified, or destroyed.
- All activities at an incident scene must be in compliance with official departmental or corporate policies and procedures.
- First responders must visually identify potential evidence, whether conventional physical evidence or electronic evidence.
- Network and telephone connections must be identify.
- The objective of an electronic forensic investigation is usually to provide digital evidence of a specific or general activity.
- Rigid recovery procedures are required when conducting computer and electronic forensic investigations.
- There are numerous situations involving corporate security issues and criminal activities that might profit from an electronic forensic investigation.
- The physical environment of the incident scene in a business setting can be quite different from a normal crime scene.

Corporate Criminal Activities

- Illegal business activities are divided into White-collar crimes and Blue-collar crimes
- White-collar crimes overlaps with corporate crimes because the opportunity for fraud, bribery, insider trading, embezzlement, computer crime, and forgery is more available to white-collar employees.
- White-collar crime can be further defined as those illegal acts that are characterized by deceit, concealment, or violation of trust and that are not dependent on the application or threat of physical force of violence.
- The types of crime committed are a function of the opportunities available to the potential offender.
- Because there are fewer opportunities to use a skill, more-blue-collar crime may involve the use of force
- In criminology, blue-collar crime is any crime committed by an individual from a lower social class as opposed to white-collar crime, which is associated with crimes committed by individual of a higher social class.
- Blue-collar crimes tend to be more obvious and attract more active police attention (e.g., for crimes such as vandalism or shoplifting, which protect properly interest), where as white-collar crimes can intermingle legitimate and criminal behaviors and those who commit them can be less obvious.
- Categories of white-collar crimes include corporate crime, state crime, and stat-corporate crime.

Preparation

- Different categories of circumstances will require a different type of response and investigations.
- If there is an allegation of internal financial fraud or theft of trade secrets, the approach will be very different that an obvious violation of a security or computer-sue policy.
- Before any overt investigative action, the activities must be coordinated with the security department, the employee's management, personnel, and possibly law enforcement.
- The nature of the complaint must be determined before any action is undertaken.
- False accusations by management can result in employment lawsuits and cause embarrassment to the organization; therefore, facts must support any action.
- If criminal activity is revealed, such as child pornography or dug trafficking, a search warrant might be required.
- If criminal activity is identified, the steps required for a law-enforcement forensic investigation will be initiated and the security organization and the corporation will lose control of the situation.

Case Categories

- Many different categories of corporate policy violations can benefit from the introduction of forensic investigations.
- Common examples might include the following:
  - Corporate espionage
  - Discrimination issues
  - Employee Internet or e-mail abuse
  - Improper accounting practices
  - Misuse of company resources
  - Pornography
  - Security and computer policy violations
  - Sexual harassment
  - Theft of company property
  - Unauthorized disclosure of corporate information and data
- Electronic forensic techniques have been utilized to assist in solving a number or petty and felony crimes. Examples of criminal activity include:
  - Capital crimes where information and data is stored electronically
  - Crimes against the state
  - Criminal fraud and deception
  - Cyber crimes
  - Cyber-terrorism
  - Etc.

Preliminary Investigation and Fact Finding

- There are a number of important issues that must be considered when corporate security is investigating an incident or crime involving computer and electronic devices.
- Two basic rules are: change nothing and record everything.
- A preliminary goal is to determine whether the incident is a true crime, failure, or an accident.
- Other considerations that might be viable are:
  - Did the incident originate from an internal or external source?
  - Is it currently an ongoing, active issue?
  - Is it an intrusion, incident, or attack that has already occurred?
  - Is it an intrusion, incident, or attack that has already occurred and is likely to occur again in the near future?
- Corporate administrator will know when a system cannot be bought down. They can help the security staff make a backup of the entire system after an intrusion staff make a backup of the entire system after an intrusion or attack and be prepared to testify to what processes occurred
- If the investigation involves the Web, there are several preliminary items of information that would be critical in the investigation. Any addressing information, such as the Internet protocol (IP) address or uniform resource locator (URL) would be important.
- All activities involved in this evidence identification must be noted in the investigator's journal.

Documenting the Corporate Incident Scene

- Documentation of an incident scene creates a permanent historical record that must stand up to intense scrutiny. Formal procedures and processes must be followed for each incident investigation.
- It is very important to accurately record specific details concerning the location and placement of electronic devices, computers, storage media, and any other convectional evidence.
- The incident scene search must be a planned, coordinated, and executed effort by corporate security personnel to locate physical evidence in support of some policy violation or complaint.
- Corporate security and computer-sue policies will dictate the type of investigation initiated.
- When a formal violating is investigated, a decision must be made about whether to confront.
- There are a number of basic documentation steps taken during the initial walk-through of the incident scene that will ensure relevant evidence is capture. These include the following:
  - Document the condition, location, and power status of any computer devices
  - Identify any storage media that might be visible around the work areas or in disk storage trays.
  - Develop an inventory of any electronic devices including cell phones and PDAs at the incident scene.
  - Identify and document any devices or components that will not be collected as evidence.
  - Produce a 360 degree photographic journal of the incident scene.
  - Collect printouts from the work area or the printer tray.
- A chain-of-custody must be maintained because of the potential for legal action.

Documenting the Corporate Incident Scene

- Documentation of an incident scene creates a permanent historical record that must stand up to intense scrutiny. Formal procedures and processes must be followed for each incident investigation.
- It is very important to accurately record specific details concerning the location and placement of electronic devices, computers, storage media, and any other convectional evidence.
- The incident scene search must be a planned, coordinated, and executed effort by corporate security personnel to locate physical evidence in support of some policy violation or complaint.
- Corporate security and computer-sue policies will dictate the type of investigation initiated.
- When a formal violating is investigated, a decision must be made about whether to confront.
- There are a number of basic documentation steps taken during the initial walk-through of the incident scene that will ensure relevant evidence is capture. These include the following:
  - Document the condition, location, and power status of any computer devices
  - Identify any storage media that might be visible around the work areas or in disk storage trays.
  - Develop an inventory of any electronic devices including cell phones and PDAs at the incident scene.
  - Identify and document any devices or components that will not be collected as evidence.
  - Produce a 360 degree photographic journal of the incident scene.
  - Collect printouts from the work area or the printer tray.
- A chain-of-custody must be maintained because of the potential for legal action.

Conducting Interviews

- Investigators may wish to conduct preliminary interviews at the incident scene.
- Witnesses, potential suspects, and others present at the scene must be identified and separated.
- Consistent with law enforcement, security departmental, or corporate policies and procedures obtain the following information and details:
  - Chain-of-command list with corresponding responsibilities
  - Documentation of any hardware and software installed on the systems
  - Location of any off-site media storage
  - Owners and/or users of any computers or electronic devices found at the incident scene
  - Passwords, logons, usernames for PCs, laptops, etc
  - Physical map of the incident scene layout
  - System passwords and logons for applications
  - System usage and purposes
  - Unique security schemes or destructive processes
- If the investigation involves the Internet, network services providers and Internet services providers (ISPs) must be identified

Identifying and Collecting Evidence

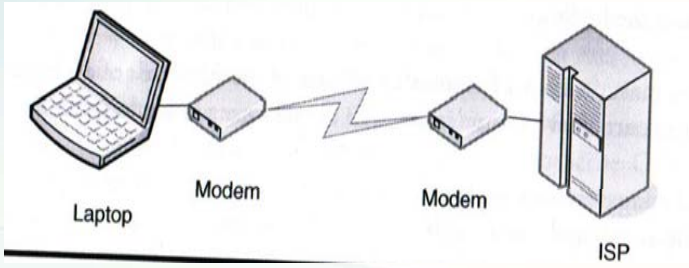
- The first person responding to an incident can make or break a case.
- Without developing advance, sound, validated, ethical and legal processes and procedures, the security team may very well lose evidence recovered while on site.
- It is essential that first responders be trained in good forensic practice as it relates to the search and seizure of electronic and computer media.
- A special note: if the device is powered off, leave it off; if it is on leave it on.
- Large departments may employ personnel who can image hard-disk drives. A number of activates must occur after copies or images have been made of the electronic evidence. A forensic examiner may perform the following:
  - Investigate data and settings from installed applications and programs
  - Look at the general system structures
  - Identify factors relating to the user's activities
  - Identify and recover all files including those deleted
  - Access and copy hidden and protected files
  - Access and copy temporary files
  - Use forensic techniques to recover residue from previously deleted files.
- A full and detailed report must be created from these investigations.

Identifying and Collecting Evidence (Cont.)

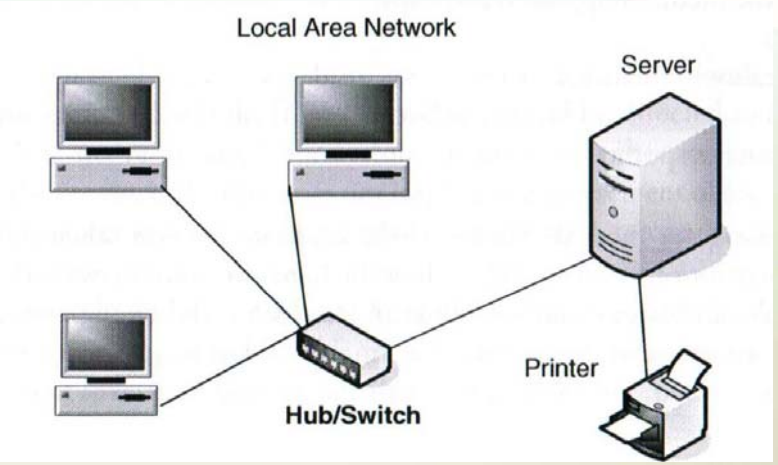
- Process must be initiated for investigating data storage devices and/or data processing equipment consisting of a home compute, laptop, server, office workstation, or removable media such as compact disks (CDs), to determine if the equipment has been used for illegal, unauthorized, or unusual activates.
- Computer forensics experts must:
  - Identify sources of documentary or other digital evidence
  - Preserve the evidence, analyze the evidence, present the findings
- They must do so in a fashion that adheres to the standards of evidence admissible in a court of law. Considerations, in the following order, include:
  - Gathering electronic evidence
  - Understanding the suspects
  - Securing the machine and the data
  - Examining the machine's surroundings
  - Recording open applications
  - Powering down carefully
  - Inspecting for traps
  - Fully documenting hardware configuration
  - Duplicating the hard drives

Stand-Alone and Networked Computers

- Most desktop and laptop computers operate in a stand-alone mode and are connected to the Internet via a communication device such as a modem.
- Evidence, however, could be located at the ISP location.



- Computers located at a business location will usually be networked. Multiple computes at a nonbusiness location might also indicate a networked environment.
- Networked systems such as a LAN will require someone who possesses specialized knowledge in the evidence-seizure phase of the investigation.
- Computer systems located at business, education, and government locations are usually interconnected with each other over some type of network.



- Advance planning should occur before attempting to recover evidence from these networked computer configurations.
- The computer network might include access to a mainframe system, servers, o just computer-to-computer connectivity.
- Be suspicious if an employee seeks to assist the investigators because this person might be involved in a cover-up of vital evidence.

Miscellaneous Devices

- A number of miscellaneous electronic devices might be present at the incident scene.
- Today technology allows almost any device to contain electronic or forensic evidence.
- Data present on these devices can be lost if no handled properly.
- *Note: Additional latent evidence such as fingerprints and fluids (DNA) might be present on any of these devices.*
- Example of other electronic devices that might provide latent evidence include the following:
  - Answering machines
  - Cell phones
  - Digital cameras
  - External disk drives
  - USB flash drives
  - Pagers
  - Removable media (floppies, CDs, Zips)
  - Telephones with features
  - Wireless access points
  - Caller-ID devices
  - Copy machines
  - Dongles
  - Fax machines
  - GPS devices
  - PDAs
  - Scanners
  - VCRs
- The investigator must determine if the organization has taken due diligence, including precautions to ensure that all of the hardware and software that is reasonable available, and is an industry standard, has been installed to prevent unauthorized instructions or use of the system.

Disclaimers that Aid Investigators

- Often information technology management is derelict in notifying users of security policies and data access security levels. This lapse can result in a case being thrown out of court, because the user can claim there were not any rules or policies on the use of the networks, computer, or electronic device.
- Each computer network and terminal should have a disclaimer that the material contained in the computer is proprietary and only for official use.
- A disclaimer is a statement denying responsibility for a particular action.
- The notice should state that the device is to be used expressly for business and that the owner has the right to search and look at anything sorted on or crated by the device at anytime.
- Two samples of disclaimers are:
  - *User of this website and its contents are at the user's risk. The website assumes no responsibility for consequences from the use of the information contained in this sit, or in any respect for the accuracy, adequacy or completeness of such information. The website is not responsible for, and expressly disclaims all liability for, damages of any kind arising out of use, reference or reliance on such information.*
  - *The links provide by this website are intended to provide a wide range of information. The links form this website could be directed to access other Internet resources, information, or procedure that are unrelated to it. The presence of a link does not imply any endorsement of the material on the websites or any association with the website's operators.*
- Investigators should determine if the incident organization has a disclaimer for computer and resource usage.

E-mail investigation

- E-mail abuse is a problem in many corporate organizations. Abusers can consists of inappropriate and offensive message content to various forms of harassment and threats.
- It is also a major issue caused by SPAM, which is defined as unsolicited e-mail messages.
- Investigator policy violations and crimes that include e-mail is similar to investigating other types of incidents that relate to computer abuse.
- If the e-mail incident involves individual that are part of the organization's internal network, the approach of the security personnel will be different from one that involves external parties.
- The investigator should take a preliminary look at evidence that might indicate a possible e-mail-related crime or corporate e-mail policy violation. Minimum information should include the following:
  - The name of the ISP
  - The offenders' name and address
  - Copy of the e-mail exists (ISP has the e-mail in the computer mailbox)
- Two considerations closely related to email are newsgroup and chat rooms investigation.
- Items of information required are similar to that for e-mail:
  - For a newsgroup: the name of the newsgroup, the name of the posting, printed copy of the screen image, copy of the posting saved on the computer or computer media
  - For a chat room: name of the chat room, name of the server where the chat room is located, identity of a nickname or screen name used, IP address used during the chat, copy of the chat dialog window or user's list, information saved to a computer or disk.

Types for Evidence

- Not all items at an incident scene will consist of electronic evidence. Printouts, handwritten notes, and photographs might be in the space surrounding the computer area.
- Items relevant to subsequent examination of electronic evidence may exist in written passwords, calendars, mail, literature, and black pads or paper with indented writing.
- The contents of the search warrant will dictate the areas where evidence can be seized.

Evidence Handling

- There are a number of issues relating to electronic and computer evidence that must be addressed to ensure proper evidence handling. Categories that ensure that evidence will be useful and valid include:

Forms and Documentations

- The name of the game is documentation and more documentation; however, it must be relevant to the investigation.
- Two forms that are presented for corporate security investigations include a journal and chain-of-custody.

Labeling and Tagging

- Computer and electronic devices and media that are collected as evidence must be thoroughly labeled or tagged and an inventory log maintained as part of the chain-of-custody.
- The task of retrieving evidence is usually the function of the forensic investigative team, who is experienced in the process required to ensure evidence is admissible in legal proceedings.

Evidence Handling (Cont.)

Protecting and Packaging

- Most corporate security departments are not prepared to follow chain-of-custody requirements.
- Employees of IT departments are generally not qualified to collect computer forensic evidence.
- Security first responders must ensure that computing devices remain untouched until a qualified forensics specialist can create a certified, bit-by-bit copy of the drive.
- After all the evidence has been collected, logged, and properly labeled and tagged, it must be packaged in acceptable containers.
- Computing electronic devices are fragile instruments that are sensitive to temperature, humidity, ,static electricity, ,magnetism, and physical shock.
- To preserve the integrity of the chain-of-custody, documentation should provide an audit trail of the packaging process.
- Serial numbers should be noted on the log form; however, it will be easier if to reconstruct the computer configurations if the serial number is also on the package.

Evidence Handling (Cont.)

- There are five basic steps for packaging computer and electronic devices. These include the following:
  1. Ensure all collected evidence is properly documented, labeled, and inventoried before the packaging process.
  2. Pay particular attention to latent or trace evidence and take the necessary actions to preserve it. Fingerprints might be on the screen or mouse
  3. Pack magnetic media in antistatic package. Avoid standard plastic bags.
  4. Avoid folding, bending, or scratching computer media, such as floppies and CDs. These components must not be exposed to magnetic fields or excessive heat.
  5. Ensure all containers used to hold evidence are properly labeled.

Evidence Handling (Cont.)

Transportation

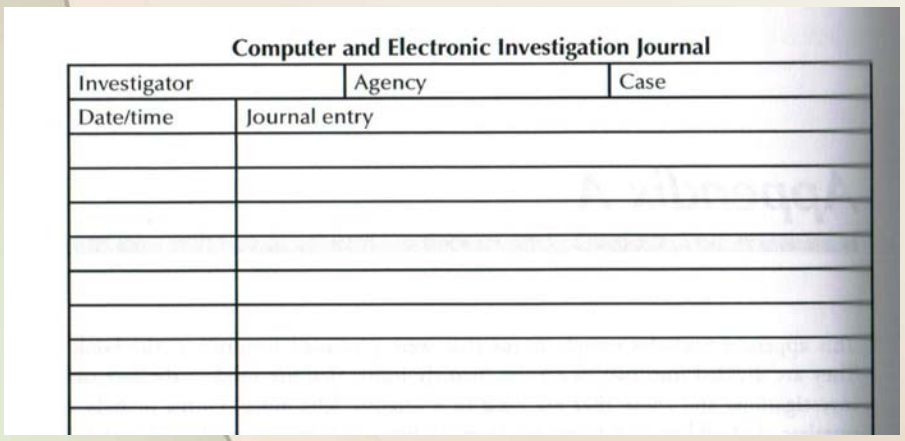
- After all steps have been taken in the packaging phase, the nest step is to safely transport all the evidence to the storage area or directly to the forensic lab.
- The transportation phase has four steps:
  - Keep electronic evidence from electromagnetic sources
  - Avoid storing evidence in vehicles fro prolonged time periods because circuits boards and storage media could warp.
  - Ensure that the computers or other devices too large or bulky to box are secured in the vehicle against shock or excessive vibrations.
  - Maintain the chain-of-custody on all evidence transported.

Storage

- The last step is to store the evidence in an approved storage area. This must be a locked, controlled area.
- There are two broad steps and one specific activity in the storage procedure. These are:
  - Ensure all evidence is inventoried in accordance with departmental policies and legal requirements.
  - Store evidence in a secure area away from any foreign sources that might reduce the importance and content of the evidence. Evidence must be protected from electromagnetic sources, moisture, dust, and any harmful contaminants.
- Appropriate personnel must ensure that devices requiring ongoing power are connected to a reliable power source.

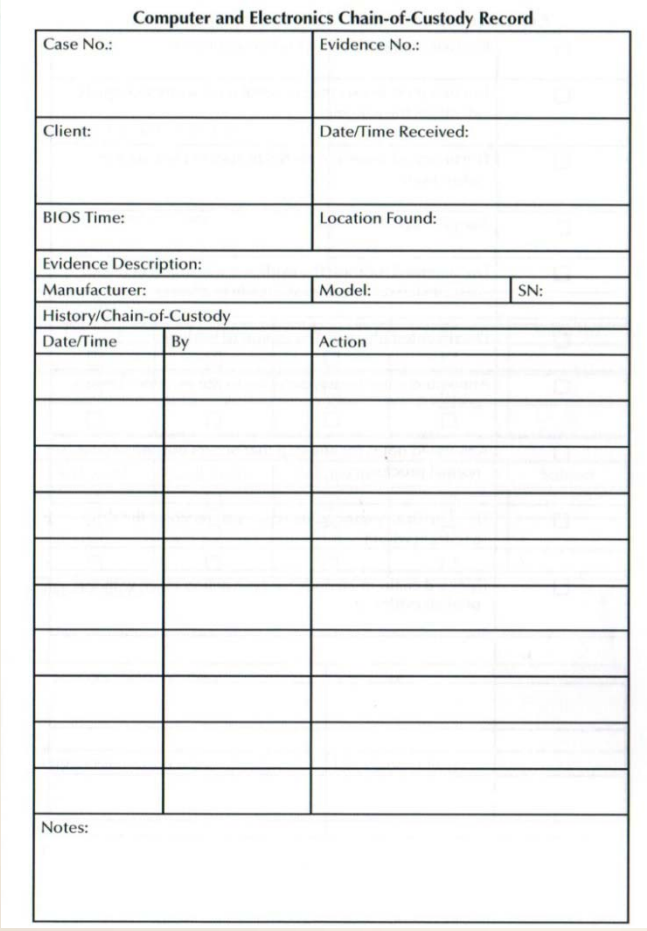
Forensic Investigation Documents

- All of the steps in the forensic investigation require some type of documentation.
- Official policies must be in place, which describe the investigative activities for these incidents.
- A number of forms can be developed to assist in these steps.
- Evidence forms include:
  - Investigation journal
  - Chain-of-custody form
  - Evidence detail log
  - Photographic log
  - Evidence receipt
- Check list include:
  - Chain-of-custody checklist
  - Evidence receipt checklist
  - Investigation checklist



Computer and Electronic Investigation Journal

Investigator	Agency	Case
Date/time	Journal entry	



Computer and Electronics Chain-of-Custody Record

Case No.:		Evidence No.:	
Client:		Date/Time Received:	
BIOS Time:		Location Found:	
Evidence Description:			
Manufacturer:		Model:	SN:
History/Chain-of-Custody			
Date/Time	By	Action	
Notes:			

Law Enforcement

- If the organization has any intention of prosecuting someone connected to a security incident, considerations concerning law enforcement involvement must be made early in the investigation.
- There are a number of law enforcements levels that are available to respond to investigate incidents.
- The incident response team must be acquainted with its various law enforcement representatives before an incident occurs.
- Law enforcement departments should be contacted through designated individuals in a manner consistent with the organization’s procedures and legal restriction.