Working with Law Enforcement

Supplement to CSH5 Chapter 61

M. E. Kabay, PhD, CISSP-ISSMP
Prof. Information Assurance & Statistics
School of Business & Management, Norwich University
mailto:mkabay@norwich.edu V: 802.479.7937

Topics*

- Background
- Goals of Law Enforcement
- History of Law Enforcement & Computer Crime
- Anatomy of a Criminal Investigation
- Establishing Relations with Law Enforcement
- Organizational Policy
- Decision to Report Computer Crime

*These notes are loosely based *in part* on CSH5 chapters 55 & 61 and also on notes from the CJ341 Cyberlaw & Cybercrime course I teach at Norwich. However, separate files will adhere to the contents of each of these two CSH5 chapters.

Background: Crimes Involving Computers

- Pedophiles
- Hate groups
- Pornography (child, adult)
- Malicious software (viruses, worms, Trojans)
- Stolen/counterfeit software, music & video
- Plagiarism
- Criminal hackers (penetration, vandalism, hactivism)
- Breaches of confidentiality (eavesdropping,
- Fraud (online sales/auctions, stock manipulation, theft of identity)

Goals of Law Enforcement

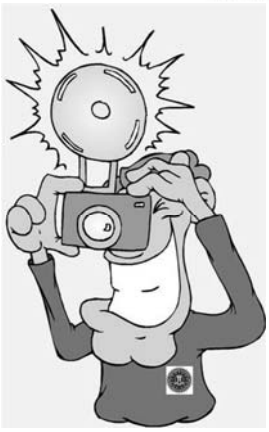
- Resolve jurisdictional differences
- Optimize use of limited resources
- Identify & prosecute suspects
  - ID perps especially hard in computer crime
  - Employee assistance can complicate task
    - ✓US: Fourth Amendment
    - ✓Employee must not act as agent of LEO
  - Involve corporate counsel at all stages
  - Prosecutor decides whether to go to trial
- Deterrence
  - Victims may suffer from publicity

History of Law Enforcement & Computer Crime

- Enforcement rule
  - Crimes often cross jurisdictional boundaries
  - Increasing cooperation
    - ✓Inter-state in US
    - ✓International
    - ✓But sometimes reduce local efforts
- Forensic examinations
  - Increasingly sophisticated utilities, police & commercial labs
    - ✓EnCase® highly popular
- Training more widely available at government, colleges
  - NU has digital forensics course
  - Champlain College has degree program

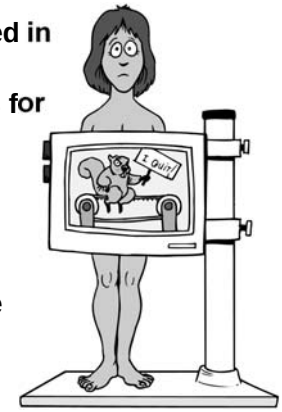
Criminal Investigations

- Anatomy of a Criminal Investigation
- Goals of Investigation
- Law Enforcement Investigations
- Problems for Corporate Investigators
- General Approach for Internal Investigations



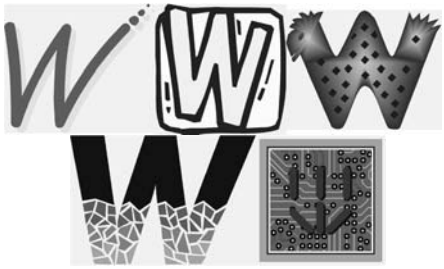
Anatomy of a Criminal Investigation

- Not all attacks are discovered in progress
- Need a well-defined process for collecting and safeguarding evidence of possible crime
- Must identify damage and initiate repair
- Critically important not to damage or destroy evidence



Goals of Investigation

- 5 Ws:
  - Who
  - What
  - Where
  - When
  - Why



And also HOW.

Practical Goals

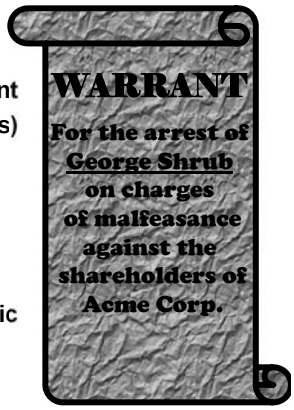
1. Understand how penetration worked
2. Get info to wiretap/trace phone lines
3. Discover motivation for intrusion
4. Collect evidence of intrusion
5. Narrow list of suspects / exclude employees
6. Document damage, including investigation and repair

FBI Approach

1. Check records (system, suspect)
2. Interview informants
3. Conduct surveillance
4. Prepare search warrant
5. Search suspect's premises
6. Seize evidence

Problems for Corporate Investigators

- Cannot prepare search warrants
- Cannot investigate outside corporate property without consent
- Cannot monitor home of suspect(s)
- May not want to result in arrest or prosecution
- May be hampered by internal politics
- Risk of employee lawsuits
- May damage public image or public relations



General Approach for Internal Investigations

1. Eliminate the obvious
2. Guess at the attack method
3. Reconstruct the crime
4. Traceback to locate source of attack
5. Analyze source, target and intermediate computers involved in attack
6. Collect evidence (maybe even computers)
7. Present evidence to appropriate authorities for follow-up

Eliminate the Obvious

- Don't assume that there is in fact a crime
- Use deduction to narrow down possibilities
  - Outsider?
  - Insider?
- Exclude suspects if possible

Hypothesize the Attack

- Collect IMAGE of victimized computer data
  - Do not power off or power on target computer(s)
  - Don't even use the target computer
  - Make exact copy of disk (& possibly RAM) using specialized utilities
- Examine log files
- Look for exploits that attack similar hardware and software as victim machine(s)
- Study access-control lists and other security barriers (who could have penetrated this way?)

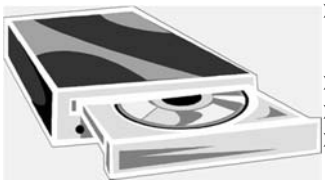
Reconstruct the Crime

- See if you can lay out exactly what could have happened during the attack
- Can use a simulated victim computer/system
  - Configure as close to identical as possible
  - Enable similar logging, security etc.
- If it is possible to achieve similar effects with a particular hypothesized attack method, this *may* be the method used
- But neither positive nor negative results will be conclusive

Traceback

- Tracing origin of Internet attack very difficult
  - IP packets can have *forged headers*
  - Many attackers route their attacks through intermediate victims
- Other problems occur because some system administrators or managers won't cooperate
  - Fear of bad publicity
  - Costs of doing investigative work
  - legal involvement or *downstream liability*

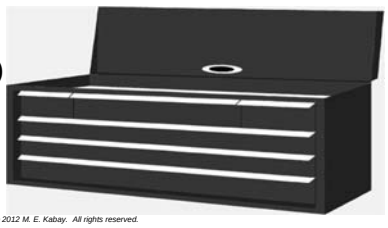
Analyze Source / Target / Intermediate Computers



- Boot PC to DOS (not Windows)
- Copy physical bit-for-bit image of entire hard drive(s) to removable media
- Burn a CD-ROM (or CD-RW) with the data
- Create duplicate drive/system on another computer
- Work with the *copied data* on that other computer, NEVER with raw/original data
- Read all log files
- Examine date-last-mod on all files
- Look for anomalies in config & startup files

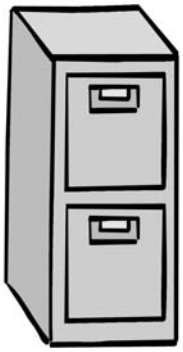
More on Analysis

- Search for known hacking tools
- Compare critical files with known-good versions
- Look for unauthorized accounts
- Search entire drive (not just files) for keywords
- Analyze all communications connections
- Verify significance of every file on disk (including erased files)

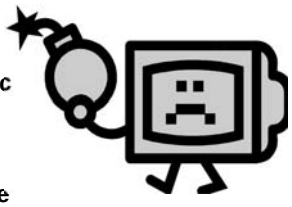


Collect Evidence

- If possible, impound the computer(s)
- Safeguard the bit-image copy of the disk: maintain *chain of custody*
  - Keep under lock and key
  - Document exactly who had access to disk at what time
  - Ensure at least 2 people present for all operations involving evidence
  - Keep paper log records of everything being done with data
  - Sign, date, timestamp, safeguard paper too



More on Data Collection from Computers



- Use expert familiar with forensic analysis of specific operating system
- Be aware of possibility of booby-traps (logic bombs) that could destroy evidence
- Never reboot computer using suspect operating system – supply external boot media
- Boot to diagnostic mode only to collect drive image
- Store media in secure and safe environment

Transfer Evidence

- Seal evidence in evidence bags
  - Signed labels over closures
  - Complete details for later use in court
- Use digital signature on all electronic data
- Prepare binder laying out the evidence
  - Number all exhibits
  - Refer to named, numbered exhibits in report
- Provide table of contents
- Write executive summary (1 page only)
- Give details of investigation
- Provide discussion of reasoning
- Show timelines

Establishing Relations with Law Enforcement (1)

- Never attack a bureaucracy without knowing
  - Who does what
  - Who has power
  - Who will help you
  - Who will hinder you
- Never try finding out about a bureaucracy in an emergency
- Therefore, get to know your local bureaucrats when you are *not* involved in an investigation
  - Get the groundwork done when you can avoid putting pressure on people

Establishing Relations with Law Enforcement (2)

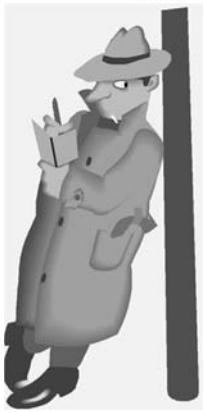
- Forge good relations *before* there's a problem
- Be aware of jurisdictions
  - Federal
  - State
  - Municipal
- Know
  - Chief of police
  - Computer-crime specialist, if any
  - District attorneys
- Offer to help in any way in other investigations if resources available

Organizational Policy

- Involve/inform/educate corporate counsel at every stage
- Communicate with LE through single channel
  - Employee release of information could taint evidence
  - Might even lead to prosecution of witness
- Preserve computer evidence
- Produce computer evidence in accordance with legal requirements and procedures only

Involving the Authorities

- Why people don't always call the authorities
- Reasons for contacting authorities
- Deciding which authorities to call
- Consequences of involving law enforcement agencies
- Deciding to call the cavalry (or not)
- Stopping the investigation



Why People Don't Always Call the Authorities

- Not serious enough to warrant nuisance
- Doesn't involve federal-interest computers
- Unlikely to reach prosecution
- Publicity could be harmful or embarrassing
- Impossible to solve
- Prosecution would cost more than reasonable
- Prosecution could cause harm to victim

Reasons for Contacting Authorities

- Computer is instrument in a reportable crime
  - Failing to report crime may be cause for prosecution as accessory before or after the fact
- Federal-interest computer
  - Involved in federal crime (gambling, kidnapping, interstate fraud)
  - Used by government or govt agency
  - Used by contractor to govt or agency
  - Used in financial industry
- Ask competent lawyer to help decide

Deciding Which Authorities to Call

- Attack on any federal-interest computer: FBI
- Threats on the President and high officials: FBI and Secret Service
- Fraud perpetrated against a specific government agency (HUD, IRS, INS, DOT, DOD, DOJ. . . .): contact *that agency*
- Critical issue is whether to use local agencies
  - If wrong level, can languish in limbo; or
  - Be thrown out of court; and
  - Preclude further prosecution because of double jeopardy
- Call a legal expert (not necessarily corporate counsel) for sound advice

Know Your Local Resources

- Make appointments with
  - Local, state, federal prosecutors or attorneys general
  - Computer crime squads
    - ✓ State
    - ✓ Federal
- Participate in local InfraGard meetings
  - Attend, mix, discuss, lecture
  - Offer to host meeting
- For list of local FBI field offices, see http://www.nipc.gov/contact.htm

InfraGard
Guarding the Nation's Infrastructure

Consequences of Involving Law Enforcement Agencies

- Loss of control over investigation
  - Commitment is to society, not victim
  - May or may not protect individual or corporate interests
  - But increasingly sensitive to needs of business
- Requirements of LE
  - Jurisdiction is appropriate
  - Crime has occurred
  - Large enough loss, danger, issue to warrant effort
  - Reasonable hope of solving & prosecuting

What to Expect from Law Enforcement

- Legal rights
  - Issue subpoenas for invasion of privacy
  - Seize computers without warning
  - Impound computers and data indefinitely
- More power in investigation
  - Tap phone lines
  - Initiate surveillance
  - Undercover officers
  - Question employees
  - Detain suspects
  - Examine records

Deciding to Call the Cavalry (or not)

- Evaluate objectives in pursuing incident
  - Beware rage / revenge / emotion
  - Need to learn enough to prevent recurrence
  - Consider possible backlash from perpetrator or from innocents accused of malfeasance
- Options
  - Handle incident internally
  - Take action in the civil courts
  - Treat as a criminal investigation

Calling the Cavalry (cont'd)

- Internal handling: risk of being seen as cover-up unless evidently serious
- Civil action: often useless
  - Perps unfindable or poor
  - Costs high
  - But may be appropriate for industrial espionage
- When you MUST call the cavalry:
  - Financial fraud of sufficient size (according to regulations and laws)
  - Threat to national security
  - Terrorism

Working with Law Enforcement

- Interview by LEO
  - Present clear picture, evidence, records
  - Must maintain proper procedures
  - Chain of custody over evidence
  - Copies of data used in forensics
- Answer all questions fully
  - Nothing is off the record
  - No way to decide to drop investigation if uncomfortable
  - Executives will be granted no special privileges

Review Questions (1)

1. Why do you have to establish policies and provide training for employees concerning investigations of possible computer crimes in your organization?
2. Why not call law enforcement the moment a computer crime is even *suspected* in your organization?
3. What does *chain of custody* have to do with corporate information assurance?
4. Enumerate the reasons that corporate counsel is essential throughout a computer crime investigation and prosecution.
5. How do jurisdictional issues complicate computer-crime investigations and prosecutions?

Review Questions (2)

6. What determines the choice between civil tort and criminal prosecution?
7. Summarize the balance of factors that can affect the decision whether to report a computer security incident to law enforcement.
8. Why do some investigations get blocked in the corporate world and how can you cope with opposition if you think that you should complete the investigation?
9. How do Internet and e-mail usage policies potentially affect internal investigations of possible computer crimes?
10. Once law enforcement agencies have begun their investigation, can a corporation readily stop that investigation? Document your answer.

OPTIONAL Homework

- For an extra 10 points
- Do some research in the Kreitzberg Library databases (NOT THE WEB) to locate information about a computer crime investigation and prosecution involving a corporation
- Write a 250±50 word essay summarizing the events with a special focus on investigative and legal issues
- Post your findings and references on the NUoodle discussion group under topic head IS342 Crime Investigation.
- Extra points for intelligent discussion of others' postings

DISCUSSION