How is Your Company Positioned to Deal With Law Enforcement?

Tim Proffitt

September 2009

GIAC GSEC, GCIH, GCPM, GSLC, GLEG, GSNA

Introduction

Scenario 1: Many security professionals believe Internet-related crime should be reported to appropriate law enforcement authorities. How is this executed while still protecting the organization?

Scenario2: Law enforcement can arrive at your door with little or no notice to seize equipment. Their primary mission is to build a prosecutable case. Cooperation with your organization may not be a priority. How can you position your organization to best deal with this situation?

This presentation will discuss recent seizures and the fall out from the investigation. We will cover objectives to protect your organization but still aid law enforcement in meeting its objectives.

FBI Seizures : Crydon

March 2009 FBI raids a data center in Dallas

- 220 servers, routers, switches, racks, power strips, eight iPods, five Xboxes, PlayStation3 and a Wii gaming console were seized.
- Data included sensitive, transactional records for companies using this datacenter.
- 200 companies affected.
- Computing equipment from the owner's home was taken.
- Over $2,000,000 seized from bank accounts.

The owner says the seizure resulted in him losing millions of dollars in revenue and put many of his customers out of business or at risk of closure.

FBI Seizures : Core IP Networks

- April 2009 the FBI seized all equipment at Core IP Networks.
- Approximately 50 businesses were affected.
- Customers denied access to seized equipment.
- FBI asked the companies to contact the FBI directly to help the investigation.
- Access to 911 was affected because some of Core's primary customers include telephone companies.
- FBI was searching for a VIOP scam perpetrated against ATT.

Quote from the owner: "**If you run a datacenter, please be aware that in our great country, the FBI can come into your place of business at any time and take whatever they want, with no reason**."

Goldman Sachs

- July 3, 2009, FBI arrested Sergey Aleynikov, a Goldman programmer, as he was attempting to board a plane.
- Aleynikov encrypted and transferred 32 megabytes of source code to a server in Germany. (*evidence revealed more*)
- Goldman InfoSec monitors and prohibits FTP file transfers from within the company. Number of transfers were initiated from Aleynikov's account.
- Using bash history, Aleynikov's account was seen to have made copies, encrypt, rename and erase files. "Bash history" was then erased.
- Goldman contacted the FBI and produced its evidence. Using FBI resources, an arrest was made and the files obtained from Germany.

Search Warrant

Under the Fourth Amendment to the United States Constitution, *most* searches by the police require a search warrant based on probable cause, although there are exceptions.

- Search warrant permits the government to enter corporate premises and physically seize any computer, data and other evidence in your possession.
- Agents can seize computers, printers, faxes, backup tapes, storage devices and traditional paper documents.
- Critical business information can be seized by agents even if this information is vital to the daily operations of the company.
- Agents may approach any employee, many of whom may not be prepared to answer questions or to sign documents on behalf of your corporate counsel.

As seen with Crydon, the FBI legally seized much more than the typical hard drive. Power strips, racks and consoles were taken for investigation.

Mindset During an Investigation

Law enforcement mindset – (Crydon)

- Law enforcement's mission is to identify the perpetrators and to build a prosecutable case. (Tipped by ATT & Verizon)
- Typically, the larger the damages, the better the case. ($1,000,000 in this case)
- Law enforcement's top priorities may not be your top priorities. (equipment from several companies taken offline)

InfoSec mindset – (Goldman)

- Protect sensitive information. (FBI stopped the exposure of the IP)
- Protect public image. (Goldman's image was protected)
- Ensure business continuance. (FBI worked with Goldman to obtain only the log files and data needed for the investigation)

What Evidence is Good Evidence?

Can the evidence be documented?

- This evidence should be concrete. In the case of Goldman, logs showed copies and transfers to a German server.

Does your team have audit trails that expose the incident?

- Goldman had BASH history that was shipped to their security event manger.

Can your team identify users, physical locations or IP addresses?

- Goldman had an IP address, workstation, time and username.

Can your team place the accused at the scene of the incident?

- Goldman was able to produce door badge logs that placed the accused at his desk during the file transfer and thus at the scene of the crime.

Preserve the Crime Scene

Once the decision has been made to call in law enforcement, what does the security team need to do before they arrive?

The CERT publishes an outline about what to preserve at a computer crime scene.

- Preserve the state of the computer at the time of the incident by making a backup copy of logs, damaged or altered files, and files left by the intruder.
- Activate auditing software / Consider keystroke monitoring (Be sure your legal warning banner precedes logon activities).
- Document the losses suffered.

Goldman did this correctly. The evidence they collected was clear and concise.

Investigation: What to Do?

According to a FBI (LA field office) 2002 Infragard presentation

- Notify corporate security and legal counsel
- Activate your incident management team
- Keep chronological log of events of everything the team does
- Activate all available audit trails and logging
- Maintain simple chain of custody
- Attempt to identify source(s) of attack
- Determine how the attack was conducted
- Record specific damages and losses ($5000 is magic number)
- Prepare / containment for a repeat of the incident

Be patient with law enforcement!

Investigation: What Not to Do

According to a FBI (LA field office) 2002 Infragard presentation

- Do not use the compromised systems before preserving any evidence.
- Do not make assumptions as to Federal jurisdiction or prosecutorial merit.
- Do not assume that by ignoring the incident, or damage to your files, that it will go away.
- Do not correspond via E-mail on a compromised network regarding the incident or the investigation.

What to Expect if You Call the FBI?

- Agents will interview key witnesses (IT Managers)
- Agents will trace the attack (subpoenas, 2703d orders)
- Agents will obtain search warrants and interview subjects (can get your data back)
- Agents will examine evidence, identify more victims, and develop leads
- Agents may offer assistance in recovering logs (can help your organization)
- Agents may seek to identify the individual responsible (possible plea bargaining)
- Agents may obtain Federal Grand Jury Indictment
- Arrest and Possible Trial (disclosure issues for your organization)

These steps do NOT occur quickly!

Business Continuity with Law Enforcement

Your management team should be considering what damage would be caused if any section of your information systems was the target of a seizure.

- Encourage onsite copying of memory and hard drives.
- Educate key employees to train them on what needs to be done for the investigation.
- Arrange for outages to take place during the most opportune time without delaying the investigation.
- Narrow down which logs and audit reports will be needed by law enforcement since this will minimize the amount of time to retrieve them
- With any data identified for investigation, the team should confirm that a backup exists.

Contacting Law Enforcement

The Internet Crime Complaint Center (IC3) is a fantastic way to file a criminal report with law enforcement.

•IC3 will submit your report to several agencies.

•The correct agency, if interested, will make contact.

•You receive case info via email.

Type of Crime	law enforcement agencies
Computer intrusion (i.e. hacking)	FBI local office U.S. Secret Service Internet Crime Complaint Center
Password trafficking	FBI local office U.S. Secret Service Internet Crime Complaint Center
Counterfeiting of currency	U.S. Secret Service
Child Pornography or Exploitation	FBI local office U.S. Immigration and Customs Enforcement Internet Crime Complaint Center
Child Exploitation and Internet Fraud matters that have a mail nexus	U.S. Postal Inspection Service Internet Crime Complaint Center
Internet fraud and SPAM	FBI local office U.S. Secret Service Federal Trade Commission Securities and Exchange Commission The Internet Crime Complaint Center
Internet harassment	FBI local office
Internet bomb threats	FBI local office ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	FBI local office ATF local office

Summary

- Law enforcement may be reluctant to share information with your team. Building a relationship with them before you have a crisis can be very important. Get to know the leadership of your local police department's computer crimes unit.
- Your organization should work in conjunction with management and with law enforcement guidelines to develop a policy.
- Confirm that you have concrete evidence before contacting law enforcement.
- Preserve the crime scene and train on chain of custody.
- Understand that a seizure can leave you in a disaster type scenario; plan accordingly.