

Incident Management with Law Enforcement

Ronald L. Mendell 2001-12-12

Incident Management with Law Enforcement

by *Ronald L. Mendell*

last updated December 12, 2001

Working with law enforcement may be the most interesting and challenging part of the computer security professional's job. Depending upon how well the professional prepares prior to a security incident, such an interaction can offer either a smooth, pleasant ride or a rough, rocky ride. This article will offer an overview of dealing with law enforcement agencies in security incident handling. It will offer some suggestions that will help to make private sector involvement with the cyber-police satisfactory and effective for both sides.

Law Enforcement's Thinking and Expertise

The mindset of law enforcement is an important factor to consider in situations of incident response. Their mission is to identify the perpetrators and to build a prosecutable case. The bigger the loss caused by an incident, the better the case for them. On the other hand, the security professional may be more concerned with protecting assets and ensuring the ongoing operation of the network and the systems on it. Both goals are laudable but not always mutually attainable; building on points of mutual interest will become the key to a satisfactory working relationship.

Police units continue to evolve with the demands of the Information Age. In the late twentieth century, they experienced the full gamut of computer crime investigation. Often assigned the task of probing crimes involving the manufacture, sale, and transport of computers and computer parts, a local (i.e., municipal) police unit handles everything from truck hijackings to "salami slicing" embezzlement schemes to child pornography. On the other hand, federal agencies such as the FBI or Secret Service, investigate matters in cyberspace ranging from espionage to computer intrusions.

A large part of their caseload, about 70 to 80%, involves commodity crime. People stealing computers and parts is the bread and butter arena for many high-tech cops. Child pornography and sex crimes via the Internet form another strong area for local police talents. In recent years, many police agencies have undergone extensive training on investigating these crimes. A

smaller percentage of their caseload involves programming-related crimes. These incidents encompass cases where internal technical staff members modify software to effect a theft or another crime. The tactics vary from altering accounting routines to moving funds to inactive accounts to creating fraudulent invoices. Local units do investigate system intrusions and cases involving computer viruses or sabotage. Usually these are cases confined to their jurisdiction. Incidents taking place across state, national, or other jurisdictional boundaries, however, fall within the purview of federal or national authorities (depending upon the country in which the incident takes place).

Generally speaking, more concrete computer crimes - such as the theft of money, the theft of commodities, or the exploitation of children - require the attention of local police. Security administrators can anticipate that in crimes such as these the police will very much be running the show. The admin's function may be to simply assist in providing evidence. Crimes of greater abstraction, such as complex denial of service attacks, virus attacks, or system intrusions may require more expertise at the federal level. In part, this is due to the fact that network-based incidents such as these tend to cross the jurisdictional lines that define the responsibilities of local authorities. In abstract crimes, the role of a computer security professional will be to consult with and assist law enforcement during the case. In either case, always be cooperative, and strive to meet mutual goals.

Corpus Delicti

In order to justify bringing in law enforcement agencies, it is necessary to have a [Corpus Delicti](#) - literally, "the body of a crime". Is there reasonable evidence of a crime? Or is there simply an event or an occurrence that can't be explained? It is crucial to rule out non-criminal causes for what has happened before calling in law enforcement. They want to investigate computer crimes, not accidents.

At the same time, all aberrations or abnormal activity may be indicative of a security incident. In his book, *The Cuckoo's Egg*, Clifford Stoll recounted that he found an accounting discrepancy of less than a dollar on his UNIX system. At face value, the problem was trivial. The cause, though, turned out to be anything but trivial. Dogged investigation by Stoll exposed international espionage. The lesson is that all anomalies must be investigated in order to identify their nature and their cause.

Assume that every suspicious computer event has an accidental cause. Then, assemble facts to

prove that theory. If you can't prove an accident, you may have a security incident on your hands, in which case you should see if you can establish intent or motive for the actions. For instance, a server can fail if someone doesn't map logs to the correct storage location. That's an accident. But if the mappings were correct and someone changed them without authorization, there may be reason to suspect a security incident. As Sherlock Holmes reasoned, "when you eliminate the impossible, whatever remains, however improbable, must be the truth."

A preliminary inquiry should include:

- Ruling out a normal hardware or a software failure.
- Developing a chronology or timetable of what happened.
- Auditing for any unusual activity during that time frame.
- Identifying any users or processes involved.
- Evaluating the motives of any actors. For an external attack, this motive may involve using a known exploit, the signature of a hacker or script kiddie. In an internal attack, the question becomes: "Who would have gained from this event?"

Case Value

One of the things to consider prior to getting law enforcement involved in an incident response is whether the case justifies law enforcement involvement? If you don't bring them in, what is the worst that can happen? Obviously, there are legal and ethical issues to consider here. For example, if discovered your FTP server harbored child pornography, you should report the incident to the police immediately. But, small losses may not be worth law enforcement's full investigative efforts.

Request that the police investigate any felony, no matter the amount of the financial loss. The perpetrators of the crime may pose a danger to the public or to other businesses and organizations. Become familiar with the computer crime statutes for your jurisdiction, so you will know what constitutes a felony offense. One Internet resource for this information is [University of Dayton Law School's Cybercrime site](#). The federal statutes are available at [CERT](#).

In computer crimes that are not a felony, consider the impact of the loss on your business or organization. Is it worth using the business's time and resources to pursue? Smaller losses may be best handled on a "report only" basis, which means that you report the incident, but don't necessarily require an investigation. Always take into account the intelligence value of any

incident. What may be small to your organization may help your local police's high-tech unit, the FBI, or the Secret Service get another piece that adds to the solution of a bigger puzzle.

Report everything that you know to be a crime at least at the CERT level. (CERT, the national computer incident center, will report incidents to law enforcement if you authorize the release of such information.) Felonies need immediate police notification. Request investigative assistance on all incidents you think will have a serious impact on your organization. What constitutes a "serious impact" requires definition by upper management and should be clearly stated in the organization's security policy and, if applicable, its incident response policy. The administrator should work in conjunction with the organization's executive and with law enforcement to develop these guidelines. A rule of thumb would be a loss greater than 1% of the business' annual net profit.

Protecting the Crime Scene

Once the decision has been made to call in law enforcement, what do the computer crime specialists want security administrators to do before they arrive? What should be done with the evidence? What logs and records should be secured? Should computer equipment that may have been involved be turned off or disconnected from the network? Should administrators begin their own forensic analysis? If physical evidence forms a part of the crime, what steps should you take to preserve it?

Security managers can best assist police by carefully preserving a crime scene. Unfortunately, the crime scene may be much more amorphous than in traditional common-law crimes. The scene may stretch across a network or even elements of the Internet. The best rule of thumb is not to alter the state of computer-based evidence, even slightly. The security staff should secure all relevant logs and files, source code records, and a copy of the object code, if available. The same goes for relevant e-mails and network system files. Local machines suspected of containing evidence need to be left untouched in their original state. Furthermore, purges of data held on involved servers must not be allowed until the police have a chance to examine the file structure.

When in doubt, don't touch that keyboard. In trying to conduct forensic examinations themselves, company security personnel, unless they are qualified experts, may create serious chain of custody and evidentiary problems for the police. Many law enforcement agencies invest about \$12,000 to train forensics officers in the basics of computer forensics. So, it is not

something an employee who's been to only one weekend seminar can handle. Not knowing how to inspect the computer properly can cause the deletion or alteration of key evidence. If you don't have extensive training, leave things alone.

The Federal Investigative Guidelines found at [CERT Coordination Center](#) provide additional counsel on what to preserve at a computer crime scene. When an incident is still in progress, CERT recommends that, "if the incident is in progress, activate auditing software and consider implementing a keystroke monitoring program if the system log on the warning banner permits."

First Notice – Search Warrant

What do you do if the first notice that you are given of a possible security incident is a law enforcement agent appearing at your office with a search warrant? Nothing is more unnerving. In order to minimize the stress involved, it may be beneficial to have a plan in place for such a situation. Security staff should understand beforehand what their rights and obligations are in such a circumstance. This should be included in the organization's security policy and can be developed in conjunction with the local legal authorities and the organization's legal department.

First, keep your cool, and stress with the search warrant team that you want to cooperate. Don't be defensive or appear to be trying to hide anything. Explain what you are doing to help. Then, do the following:

1. Read the warrant carefully to find out what they want to search or seize.
2. Notify upper management and the legal department about what is happening.
3. If the authorities are wanting to search a local machine, the impact on the organization may be minimal. Get the appropriate manager or supervisor in to evaluate the impact and to assist the officers in securing the machine. In cases of child pornography, the police may need to take the entire computer. If so, work with them to see if backup copies can be made of critical data and programs prior to removal.
4. If a server is the target, see if copies of relevant portions of the hard drives will meet the team's needs. If not, involve your server and network administrators with police in bringing down the server in an orderly fashion. The plan should also include bringing online any backup server.
5. Rarely will an entire network have to be taken down. Have your network administrator

work with the police on orderly access to parts of the network described in the search warrant.

6. After the search and seizure, the team will leave you "an Officer's Return" on what property was seized. Retain this document for review by your legal staff. Make arrangements with the team to follow up with them on the status of your equipment. Offer whatever technical assistance to law enforcement that your legal department deems advisable.
7. Meet with your management, legal counsel, and technical staff after the team leaves to assess the impact of the seizures on your operations. Also, consider what actions need to be taken for continued operations.

Keeping Your Operation Running During an Investigation

Any investigation involving continued police presence requires time and resources to support. It is important to anticipate such an occurrence and to plan how to cooperate with law enforcement without shutting down your operation. For the most part, computer crime specialists can generate data dumps, make secure copies of files, and create logs without carting away all of the organization's computers. Administrators should have a plan in place to allocate those resources in a manner that will avoid – or at least minimize - disruptions in business operations: The following is a list of suggestions that will help to minimize the disruption caused by an on-site investigation:

- A. Schedule meetings with, and participation by, key employees to take place during non-critical work periods if possible.
- B. If parts of the network need to come down, arrange for this outage to take place during non-peak hours.
- C. Try to identify at one time which logs and audit reports will be needed by law enforcement. Doing this will minimize the amount of staff time necessary to retrieve them.
- D. Make sure the police do not take software or database files for which no copy or backup exists. Prior to this, and as a matter of policy, ensure that all organizational employees and contractors are following required backup and copying procedures to avoid any unnecessary loss of vital data.
- E. Keep the investigation compartmentalized, on a need-to-know basis. This action will reduce the amount of staff involved and protect the investigation.
- F. Keep the lines of communication open with law enforcement. Knowing about the needs

for records or access to information systems in advance can save staff time and system downtime.

- G. Encourage onsite copying of memory and hard drives. Computer forensics specialists possess this capability, and not all cases require the removal of equipment to a forensics lab. And with police cooperation, you can schedule these procedures during non-peak hours and keep your equipment on the premises and in service.

Non-Electronic Records

Paper records and video surveillance tapes can play a major role in investigating computer crime and incidents. As up to 85 percent computer crime are thought to be committed by insiders, internal documentation becomes important evidence. For example, if video cameras monitor the entrances to the computer processing center or labs, the video surveillance tapes produced document who entered and exited at a given time. If the entrances use access cards, the reports or databases containing the access transactions document employee traffic into sensitive areas.

Looking for contradictions between access and video records will often document something amiss. For example, if the access control report shows John Jones entering the computer lab at 6:45 p.m. on 07-01-01, but the videotape for same time shows Sam Smith entering, then Sam has used John's card or access code.

Paper files such as personnel records, departmental documents, project logs, programming modification records, sign-out logs for software, and job assignment records all tell a story. When you want to know who worked on what or who had access to which project, paper records often provide the needed history.

A tendency to think of computer crime as something external often creeps into security thinking. The brutal truth remains most computer crime is internal. And, a certain amount of that crime will be cold cases, crimes that get discovered a long time after they occurred. In investigating cold cases, investigators quickly discover that employees have left, software has changed or is no longer in use, and people's minds rapidly fade in remembering who did what. Paper records from projects may be the best evidence available in cold cases.

When examining paper records or videotape, maintain a database of what you have examined and any cross-references against other records. If you supply records to law enforcement,

make an entry of those documents in the database. Such a record will prove to be an invaluable resource in quickly locating information in an investigation.

Building Cooperative Relationships

Law enforcement may be reluctant to share information with you, an outsider. So, start building trust with them before you have a crisis. As suggested earlier in this article, work in conjunction with local police to develop incident response policies. Get to know the leadership of your local police department's computer crimes unit. If you belong to a local technology association or computer security organization, contact the public affairs office of the police, and arrange to have a speaker come to your group. Get involved in networking through your local chapter of ASIS (American Society for Industrial Security, <http://www.asisonline.org/>) and the HTCIA (High Technology Crime Investigation Association, <http://htcia.org/>). And, of course, attend conventions and seminars on computer security where you meet law enforcement and get to know them. But most important, if law enforcement calls for help on a case, try to give them a helping hand. Cooperation is always a two-way street.

Ronald Mendell is an independent writer specializing in investigative and security topics. He currently does technical support for a high-tech company in Austin, Texas. He also reviews computer security titles for www.securitymanagement.com.

Relevant Links

[Introduction to the Field Guide for Investigating Computer Crime](#)

Timothy E. Wright, SecurityFocus

[SecurityFocus Forensics Mailing List](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus