

Calling the CyberCops: Law Enforcement and Incident Handling

Robert G. Ferrell 2000-04-25

A velvety darkness enfolds the room. From somewhere just on the edge of awareness a strange, rhythmic pulsing disturbs your sleep, yanking you rudely into the conscious world. For a few unreal moments you are disoriented and anxious, until your brain processes the sensory information flooding into it and reaches the conclusion that your beeper is going off. After scrambling madly in the dark, knocking over your bedside lamp, you eventually retrieve the offending little box and peer blearily at its antiseptic charcoal-on-gray message.

It's now 3:00 AM and you're sitting at a console in your computer room at the office, staring at a new directory named "ADMROCKS." You've been hacked. Your personal data space has been violated. Some nameless script kiddie has made a mockery of your well-laid security plans. What are you going to do about it?

History suggests that you'll clean up the mess, file a report with your boss, and maybe, if you're particularly community-minded, post some sanitized logs or exploit scripts to a public computer security forum such as the Security Focus "Incidents" mailing list. I mean, there's no point in calling the cops, right? They can't or won't do anything about it, right? Isn't that what you read all the time in news stories and in complaints posted on the Internet?

To a certain extent, there is some truth to this assertion. There are many thousands of computer intrusions reported each year, and their numbers having been growing far more rapidly than the staffing and training efforts of law enforcement agencies have been able to accommodate. Life is like that sometimes. Does this mean it's pointless to report your breakin to the cops? Of course not. It just means that you need to optimize the quality of the data you provide to them, in order to maximize the chances that they'll be able to help you. Garbage in, garbage out applies here as surely as it does to virtually every other aspect of IT operations.

Most of what we know, or think we know, about cops is based on television shows and movies. Law enforcement is a perennial favorite topic of the entertainment industry, and portrayals run the gamut from self-sacrificing throw-yourself-on-the-live-grenade types to amoral robotic enforcers to frankly evil psychopathic criminals. Law enforcement agents have power to curtail our liberty, or at least ruin our day, and so we either fear or envy them (depending on whether or not you want to be one). Fear breeds loathing and mistrust; envy just breeds more envy. These are marketable emotions from Hollywood's point of view, so it doesn't take much of a

conceptual leap to see why it is in their interests to exaggerate the potential for scandalous conduct by officials of the public trust.

The truth is, as it often turns out to be, far less interesting. Cops are just people; they make mistakes, feel impatience, cut corners, daydream, overlook things, and generally behave just like every other human being on this hapless planet. There is nothing that can be or, in my opinion, should be done about this. I like to believe that I'm dealing with other human beings, fallibilities notwithstanding; I'm more comfortable among my own kind. People who never make mistakes give me the heebie-jeebies. But hey, maybe that's just me.

Swinging around once more to the question of whether or not to involve the authorities in your IT crime scene, think about this: are you (and your senior management) willing to provide the resources, both in terms of technical expertise and downtime of the affected system(s), necessary for any chance at a successful investigation and prosecution? Remember that the purposes for which law enforcement agencies exist, as all of us my age or older know from watching "Adam-12," are to 'serve and protect.' Protect people and assets from assault, serve by pursuing and delivering suspected lawbreakers to the judiciary establishment for trial.

Obviously once you've been hacked it's a little late for the 'protect' part, so we should shift our attention to 'serve.' The police will serve you by investigating the crime and, if possible, bringing the responsible party/parties to justice, but only if that's what you want them to do. You're the one who has suffered a loss; you're the one who needs to initiate the process of recovering from that loss to the greatest extent possible.

Corporate entities in a capitalistic economy are concerned primarily with profits, and only those actions which in some way enhance the ability of the organization to generate those profits are likely to be supported. Don't forget this simple maxim when you contemplate what actions to take following a system compromise. The urge for vengeance may be strong, but if it doesn't make sense fiscally, it probably ain't gonna happen (unless of course you own the company, but that's rather rare for a computer security manager. If you are the owner/CEO of the company, you can skip all this philosophical stuff and go straight to implementation. The rest of us will catch up to you there).

In summary, if you want to snag the dude (or, more importantly, if you want anything done to the dude once he's collared), you need to call the cops. Of course, your insurance company might be also interested in documentation of the incident, as might any of a number of other

departments, divisions, task forces, and interest groups in some way connected with your organization. However, if do you call the cops, be prepared to give them something to work with.

Thinking like a Cop

Now let's switch roles. You're a detective on a metropolitan police force. In college you majored in accounting and minored in criminal justice. You work mainly on white-collar crimes: bank fraud, embezzlement, stuff like that. The Lieutenant calls you into his office.

"Sit down," he says, "The department's been taking a lot of heat lately because we don't have a dedicated cybercrimes squad. As of today, you are that squad."

You look at him blankly.

"Next week you take a beginning course in Unix, then the week after that one on computer security."

You stand up to leave.

"Oh, and here's your first case...some hacker broke into XYZ Company last night. Get on it."

Sound like a script from a bad cop show? Nope, it's real life. This is more or less the way a lot of computer crimes detectives got their start. Is it the best way to generate cybercops? Maybe not, but often it's the most expedient from a police administrator's viewpoint. In writing about the problem of producing cops that know computers well enough to understand cybercrimes, I coined the phrase "[If you need something that barks and flies,] It's a lot easier to train a parrot to bark than a dog to fly." My point in employing this somewhat labored metaphor is that police work, for all its complexity, is much easier to pick up than the extremely esoteric knowledge needed to plumb the depths of buffer overflows, IP address spoofing, and man-in-the-middle attacks. Most really successful computer security experts have spent years sitting at consoles, hacking away at operating system kernels and coding nifty little utilities for this problem or that. They just can't teach that during the three months or so at the Police Academy.

Be that as it may, most agencies have been forced by budgetary or administrative circumstances to assign minimally computer-savvy investigators to their computer crimes

squads. Most officers will therefore be somewhat at a disadvantage if you expect them to come in and know exactly what steps to take to secure evidence from your specific machines and network. Having a cooperative, extremely knowledgeable company representative such as a systems administrator working closely with the investigator is really essential for maximizing the efficiency of the data-gathering phase and minimizing the downtime of involved systems.

Imagine yourself in the cop's shoes, and provide support for the investigation accordingly. Peace officers are public servants, paid from tax revenues, so it makes sense from both a fiscal and a logistical point of view to make things as easy for them as you can. Your goal as the complainant should be to facilitate the investigation; the hardest task the officer should face is tracking and arresting the criminal, not getting access to and gathering usable evidence from the crime scene.

Law Enforcement's Role in Computer Security Incident Handling

Computer crimes are just that: crimes. Violations of existing law. Conceptually they differ little from any of the other so-called "white-collar" crimes, except that they frequently involve perpetrators who have no physical presence at or even near the crime scene. The usual physical evidence relied upon by forensics analysts, such as fingerprints, footprints, tire marks, signs of forced entry, traces of DNA or bodily fluids, and so on, is conspicuously absent when the crime was carried out from tens, hundreds, or even thousands of miles away.

The task of any investigator is to collect as much evidence as can be found at the scene, analyze that evidence for clues to the perpetrator's identity, and then follow up on leads generated by this analysis. When no direct physical evidence exists, inferential evidence, or evidence that some aspect of the system has been modified as a direct result of the intrusion, is the primary source of clues.

Just as in the case of physical breakins, however, the exact nature and positioning of evidence can be crucial to unraveling the chain of events. Time stamps in logs, records of network activity, new directories and files created by the attacker, incoming/outgoing mail or other packets during the period when the intruder was actively exploiting the system; all of these are important pieces of the overall puzzle. It is important to remember that any change made to the system prior to the arrival of the investigator(s) may obscure or even erase vital forensic information. Under most circumstances, the best thing you can do is to take the box off the network and leave it alone.

What's in it for Them?

Why should law enforcement care about your breakin? The answer to this question may seem obvious (that's what they're paid to do), but consider this: police departments generally get their funding based on the number of cases they handle, and often on the number of cases they successfully prosecute. Some agencies have a minimum loss/damage dollar value below which the prosecuting attorney's office won't bother to pursue a conviction. There are simply too many crimes and not enough resources to devote the same level of effort to each one. This is just a fact of life in any society without unlimited manpower and money (and if you know of one that does not belong in this category, please tell me about it).

The primary benefits of involving law enforcement are twofold:

1. You get legal documentation of the event and of your response to it;
2. You initiate a process that may benefit not only your organization, but others who have been or will be hit by this same perpetrator.

The police, on the other hand, look for cases where evidence of sufficient quantity and quality exists that there is a reasonable chance of finding and prosecuting the perpetrator, and for documentable loss that meets or exceeds their mandated minimum value. If you can provide the 'raw materials' they need to justify their involvement, they're a lot more likely to accept your case and pursue it with the vigor it needs for a successful conclusion. That's not to say that they won't even show up if you don't meet these criteria; I simply suggest that the easier you make it for the investigators, the more likely they'll be able to do the job you ask of them. Common sense is just as useful now (but a lot less common, alas) as it was in Thomas Paine's day.

How They View You

As I have taken pains to point out, the folks that are going to show up at your door in response to a report of criminal computer activity are only human. Just as you have preconceptions about them that may or may not change based on your mutual interaction, so they have them about you.

Of course, the nature of any such preconceptions may vary widely by geographical, occupational, or operational identity, as well as (and probably most importantly) according to

previous encounters experienced by the investigator(s). If you're a Computer Security Manager at XYZ Corporation and Detective Smith had a very difficult time dealing with your predecessor, or even with your counterpart at a rival company across town, chances are he's not going to be looking forward to your investigation. That doesn't mean he won't be pleasant, or that he won't do a good job--just that he will have his defenses up during at least your first meeting.

You can go a long way towards ensuring a smooth cooperative effort by being professional, cordial, and respectful. Despite what seems to be the prevailing attitude on the 'net these days, most cops aren't out to get you unless you're a criminal. They are professionals, just like you, and appreciate being treated that way. The Golden Rule hasn't lost any of its relevancy.

When to Report, How to Report

As I hope I've established by now, you will have to make the call whether or not to report the incident. If you choose to report, make certain that this decision has been approved and is supported by senior management, or else prepare to get broadsided. CIOs, CEOs, and other three letter executive types don't like to be the last to know about anything that concerns their company, especially where governmental agency involvement is concerned. Any litigation or media coverage resulting from an event needs to be handled by the legal and public relations folks, respectively; to be effective at their jobs, they'll also need as much heads up as you can provide. Dealing with a computer intrusion is really no different than dealing with a physical breakin, with the same considerations and pitfalls. The crime scene needs to be secured as quickly and as tightly as possible, all evidence should be preserved intact, and everyone not directly involved with the investigation should be kept out.

In a complex network environment containing multiple levels of trusted hosts and shared file systems, just finding all the "prints" left by an intruder can be a daunting task. The more familiar you are with and the better documented is your existing system, the easier it will be to determine what, if anything, was modified, deleted, or installed by the attacker. This information is vital, for several reasons. For one thing, it is necessary for making anything like an accurate estimate of monetary damage resulting from the attack. Secondly, the more complete your knowledge of the state of the system, the simpler the task of restoring it to an identical condition (from those copious backups you'd better have made) becomes. Additionally, if you expect to reconstruct a crime in order to understand it, you have to know what the place looked like before the crime was committed.

Much of what follows is going to be necessarily US-centric (because that's where I live), but the general concepts should be extendable more or less intact to any nation where computer crime is likely to surface. Laws and procedures vary, of course, but the basic precepts for investigating and prosecuting crimes are remarkably similar throughout much of the world, because people are people and computers are computers, no matter where they happen to call home.

There are at least six distinct U.S. federal agencies that have jurisdiction over some type of Internet-related crime: The Federal Bureau of Investigation (FBI), the Secret Service, the Customs Service, the Bureau of Alcohol, Tobacco, and Firearms (BATF), the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC). According to the publication "How to Report Internet-Related Crime," a product of the Computer Crime and Intellectual Property Section (CCIPS) of the U. S. Dept. of Justice, computer intrusions should be reported to either your local FBI office, the National Infrastructure Protection Center (NIPC) at (202) 324-0303, or your local Secret Service office. Depending on your circumstances, you may wish to involve local law enforcement authorities as well, although chances are good that the ultimate responsibility for the investigation will end up at the state or federal level, since a great many intrusions cross multiple political boundaries.

One of the best ways to ensure that your interactions with law enforcement will be of optimal benefit to both sides is to establish a rapport with the people responsible for computer crimes in your local area before any crimes are committed. Talk with them--find out what they would like to see from you in the event of an incident, and get their take on the proper way to collect and preserve evidence. After all, they're the ones who will have to make use of that evidence in both tracking and prosecuting the perpetrator(s).

The Pros and Cons of Involving Law Enforcement

Deciding whether or not to report can be a complex issue in itself; there are many aspects to consider. Some of the questions that you might want to ask yourself are:

1. How much loss was suffered (and how easy will it be to quantify)?
2. How long ago did the intrusion take place (i.e., how "warm" is the trail)?
3. Do you have complete and unaltered copies of all relevant logs?
4. Is your firm willing to pursue the matter, understanding that the costs may not be insignificant (salaries, backup media, downtime, court appearances, etc.)?

An additional consideration should be that if any of the logs or files needed as evidence contain proprietary or otherwise sensitive information, that information may become a matter of public record during the course of the trial.

One last note: for better or worse, some companies will avoid pursuing an investigation because they have something to hide (or think they do). If your senior management has been involved in any activity that they feel might appear to be incriminating, they may forbid you to bring in law enforcement with little or no explanation. There isn't much you can do about this; you must remember that as a computer security person you usually don't own the data you're protecting. It is management's call, and you will probably have no choice but to go along with whatever they decide.

Following Chains of Command

Any involvement of an outside agency, particularly of the law enforcement variety, is something that most companies control very tightly. Few things will get you in hot water faster than calling in the cops without following the proper chain of command. Any decision to involve an outside organization in the affairs of the company must be reviewed, approved, and supported by senior management. This is doubly true when that organization is governmental in nature, and triply so when it is law enforcement. As I've indicated above, some companies will have to weigh the potential benefits of bringing in law enforcement with the potential risks of having something uncovered they'd rather keep as a company secret. This is not limited to 'hanky-panky;' often proprietary or otherwise business-sensitive information is brought under public scrutiny at a trial. It may even be a strategy of the defense to subpoena information which the company may not want revealed, simply to throw a monkey wrench into the works and cause management to reconsider its commitment to pursuing prosecution. In this instance, as in all others, be certain to CYA.

Collecting Admissible Evidence

To have any chance at all of obtaining a conviction once a cracker is caught, the prosecution will need evidence that is admissible in court. The details of what can and cannot be admitted into a court of law are complex, and vary from country to country; they are outside the scope of this discussion. For our purposes, only a few general guidelines need to be mentioned.

The principal evidence you will probably have will be in the form of logs. It is critically important that you pay heed to the wording of the rules in force in your country governing the use of logs in a trial. For example, U.S. Code Title 28, Section 1732 (28 USC 1732) dictates that copies of logs are admissible, so long as the original logs were made "in the regular course of business ." In a related vein, Rule 803(6) of the US Federal Rules of Evidence states that logs (which might otherwise be considered 'hearsay') are admissible so long as they are "kept in the course of a regularly conducted business activity." This means that you'd be much safer to log everything all the time and deal with the storage issues, rather than try to turn on logging only after a breakin is suspected. Not only is this a bit like closing the barn door after the horse has fled, it may render your logs inadmissible in court.

Any physical object involved in the investigation, be it disk, tape, CPU, CD-ROM, keyboard, right down to the power cord, must be handled in strict accordance with Chain of Custody rules. Essentially this means that all items must be tagged, stored in sealed containers, and the identity of every person who has handled or been responsible for them since they were collected as evidence, along with the date and time, recorded on the label of the container. They must never be left alone in an unsecured location, or otherwise placed in any circumstance where tampering by unauthorized persons is likely to occur. This may seem like a bit much to ask in some circumstances, where many things are happening at once and it is easy to lose track of where things are and who has them. However, a reasonably sharp defense attorney will be quick to pounce on violations of chain of custody rules; if the evidence that is rendered inadmissible by this action is essential to the prosecution of the case, you are SOL. Always err on the side of being too safe and too careful when it comes to evidentiary procedures.

Cyber Crime and the Courts

The interpretation of new laws by the courts is an ongoing and highly dynamic process. Cyberindustry and its attendant cybercrime has, relatively speaking, only recently leapt out from behind a rock and said 'boo' to the judicial system, so crafting, implementation, and final interpretation of computer crime-related legislation is really only in its fractious infancy. It is unlikely that any consistent patterns will emerge until each of the broad areas of legislation has been dragged through the courts (especially the appellate process) a few times.

Meanwhile, it would be prudent to keep abreast of cases being heard and familiarize yourself with the decisions and rationales being issued on an increasingly frequent basis. With the

geometrically expanding influence and pervasiveness of the Internet-based economy, every decision that comes out of a computer-related trial is going to carry a great deal of weight, at least until legislation begins to keep pace with the technology. I won't even begin to predict where the legal landscape will stabilize regarding computer crime; you'd have better luck predicting the next lottery winner.

If you figure out how to predict the next lottery winner, however, drop me a note. Maybe we can work something out.

[Robert G. Ferrell](#), CISSP, is the Information Systems Security Officer for the National Business Center of the U.S. Dept. of the Interior. He is also active as a Perl Monger, an Internet Technologist, and a member of the [Net Wits](#). He has been involved with (primarily Unix) systems programming, administration, and security on and off since 1977.

Relevant Links

[FBI Homepage](#)

Federal Bureau of Investigation

[NIPC Homepage](#)

National Infrastructure Protection Center

[CCIPS Homepage](#)

Computer Crime and Intellectual Property Section

[Privacy Statement](#)

Copyright 2006, SecurityFocus