Payoff

Law enforcement agencies have dramatically improved their ability to handle computer crime cases. They can be the key not only in prosecuting criminals and obtaining restitution, but in deterring potential criminal activity as well. This article discusses whom to call when criminal activity is suspected, how to gather evidence that can stand up in court, and how to work effectively with law enforcement during an investigation.

Introduction

Information systems and security managers know that preventing problems is the key to their jobs. But no matter how effective their prevention programs—no matter how well they practice and preach “secure computing”—IS and security managers must be just as ready to respond when computer crimes do occur. That is sometimes easier said than done. There are many reasons why IS and security managers have hesitated to report computer crimes to law enforcement as readily as they would call 911 to put out a fire.

Depending on the type of computer system for which they are responsible, IS or security managers may be sorely tempted to try to contain the damage by themselves as quietly as possible (with the hope that some self-help measures will avoid future problems). The last thing they want is packs of law enforcement agents and prosecutors making their lives more difficult than they already are. They also do not need more questions about a security breach from customers, competitors, and the front office.

If someone is committing crimes in the computer system, why then is it a good idea to call law enforcement? Who should be called? And what would the ensuing investigation be like? This article answers these questions.

Why Call Law Enforcement?

The primary reasons for calling law enforcement when an intrusion is suspected are deterrence and restitution. Two types of deterrence can be distinguished: specific and general deterrence.

Specific Deterrence

Perhaps the clearest reason to call law enforcement when any crime occurs is quite simply to catch the criminal and deter him or her from committing more crimes. In today's high-tech world, IS managers are prone to throw intruders out (if they can) and then bar the door. Case closed. But this fairly feudal way of looking at law and order does not stop the criminal from coming back to have a try at another system.

Perhaps it is also natural that technologically minded people should regard computer crime as primarily a technological problem, rather than as a law enforcement problem. But as experience repeatedly teaches us, computer security has both technical and human elements—and no system designed or used by people can be thought invulnerable. No
matter how good a prevention program, a criminal who is smart or persistent or lucky enough can always break in—technology alone will not solve the problem.

Moreover, with computer criminals in particular, each arrest and prosecution can have an especially dramatic effect. This point is one of the interesting facts that appears to be emerging from an ongoing psychological study of computer criminals recently begun by the Federal Bureau of Investigation and the Department of Defense. Although researchers have, as yet, only interviewed a few people convicted of federal or state offenses, the preliminary statistics are revealing. At the time of arrest, each one of the subjects had already attacked, on the average, more than 150 victim computer systems and had committed more than 4,000 separate intrusions. Untold damage could have been prevented had the first victim complained the first time an intrusion was detected.

Indeed, those who do have the courage to complain publicly about an attacker often discover that they are not alone. For example, when a large aircraft manufacturer reported computer intrusions last year to the FBI, the investigation showed that the same intruders had also penetrated a federal courthouse computer system—unbeknown to its systems manager. With the cooperation of both victims, the FBI made its case—and the attackers pleaded guilty in federal court.

Finally, the importance of responding legally as well as technically to computer intrusions has grown because of the changing nature of those intrusions. Once upon a time, hackers were often thought to be adventurous pranksters, looking only to test the limits of their equipment and their own ingenuity. They were interested in impressing their victims—not hurting them—with their skill and cunning. But those days are gone, in large measure because today's computer invaders are rarely benign technical wizards. They intentionally crash systems, sell other people's credit reports, manipulate phone service, trade stolen credit card and telephone access codes, wiretap, extort, steal, and spy. Whether called hackers or crackers, these individuals are criminals who deserve to be punished for the crimes they commit.

**General Deterrence**

Another important reason for prosecuting computer criminals is that prosecutions are public statements that victims of high-tech crime refuse to take it any more. Although some criminals never consider the possibility of getting caught, most will be deterred if punishment looks at all likely. Right now, many computer criminals believe that the chance of being arrested, prosecuted, and punished is so low that there is effectively no criminal sanction against hacking. They are confident that both victims and law enforcement lack the skill and the will to hold them criminally accountable. If this attitude is to change, victims and law enforcement must demonstrate to would-be computer criminals that the odds of being punished have changed. Perhaps just as important, prosecuting computer criminals helps to teach the larger community that, contrary to popular impressions, there really is no such thing as a harmless computer intrusion.

**Restitution**

As IS managers know all too well, being the victim of computer crime is almost always expensive. Even if the intruder did not steal or damage any data—indeed, even if he or she meant to do no harm at all—the cost of resecuring the system and checking data integrity can be staggering. The aircraft manufacturer mentioned earlier spent thousands of dollars to ensure the integrity of its avionics data. In another case, a state university that provides supercomputer services for the Department of Energy lost $10,000 of billable
computer time to two invaders who ran cracker programs on the supercomputer. With the assistance of several victims (both university and corporate), the FBI made a case against both intruders—who pleaded guilty to felonies in federal court. Although none of the defendants in either case will serve time in prison, all of them were ordered to pay thousands of dollars in restitution to their victims. And, as a term of probation, their use of computers was restricted.

**Contacting Law Enforcement Authorities**

As with all criminal investigations and prosecutions, computer crime cases may fall under the jurisdiction of the federal government, one or more state governments, or all of the above. So the first question in contacting law enforcement authorities is whether to call state or federal investigators.

The federal government and virtually all state governments have passed laws prohibiting various kinds of computer crimes. Under the federal statutes, federal prosecutors have broad tools to convict electronic criminals. These include most notably:

- 18 USC § 1030 [computer fraud and abuse].
- 18 USC § 1343 [wire fraud].
- 18 USC § 1029 [access device fraud].
- 18 USC § 2510 [the federal wiretap statute].
- 18 USC § 2701 [stored wire and electronic communications].

Although the states vary widely in their legal approaches to computer crime, most have a statutory framework for prosecuting electronic cases. For that reason, IS managers should become at least somewhat familiar with the provisions of the local criminal code in this area.

Further, even though the federal statutes listed previously apply to electronic crimes, it is important to remember that federal jurisdiction is often not as broad as state jurisdiction. This is true because the particular crime must have a federal connection before federal authorities can take a case. With computers, this federal connection may arise from the nature of the victim computer—for example, a computer owned or operated by or for the federal government or a federally insured financial institution. More broadly, federal law enforcement has jurisdiction if the offense crosses state lines—if it involves two or more computers that are not in the same state. Of course, it is difficult to know at the beginning of an attack whether the attacker is inside an organization's building or out of the country. But because of the nature of communications and electronic crime, hackers commonly weave across jurisdictions, hitting targets all along the way. Federal authorities can help determine whether any particular hacker has committed federal crimes in a particular system. If not, the agents will refer the case to the correct state authorities.

Another practical restriction in federal law enforcement's jurisdiction is its limited process for dealing with juveniles. The vast majority of juvenile crime is handled by state authorities, who are in a much better position (both legally and practically) to fully address the offender. Even if federal law enforcement agents are already working on a case, discovery of a juvenile attacker is best referred to the state. But whatever the initial point of
contact, state and federal authorities have a good record of working together in computer cases and call on each other for help in many ways.

IS managers who wish to begin a case with federal investigators have two options. Both the FBI and the Secret Service have investigative jurisdiction, and either of their local offices may be contacted. These two agencies also have investigators in the Washington DC area who specialize in electronic crime cases and who investigate computer crimes and consult with field agents across the US. The Secret Service and FBI have an agreement (called a Memorandum of Understanding) about which agency will take the lead in certain given areas, and they have also worked on several cases jointly. Therefore, it is no problem when a case needs to be referred from one agency to the other, and the investigators will handle the transfer. As a practical matter, the Secret Service has tended to specialize in fraud cases involving financial institutions, credit cards, or cellular telephones. But if working one of the two is more convenient or more familiar, initial contact can be made with that agency.

Gathering Evidence with Care

Although IS managers and systems operators are the experts on their particular systems, most are not experts in collecting and preserving evidence for criminal prosecutions. They should therefore be careful about trying to collect and analyze electronic evidence for a case.

Both federal and state courts operate under strict and formal rules of evidence that control what judges and juries can consider as proof. The Federal Rules of Evidence prescribe what may or may not be admitted as evidence in federal trials, no matter who collected it in the first place.

Every time trial lawyers offer any piece of evidence in court, they must be ready to “authenticate” it—that is, to show that, as stated in the Federal Rules, “the matter in question is what its proponent claims.” One of the most common methods for authenticating evidence is to show the item’s identity through some distinctive characteristic or quality. Indeed, if an item is distinctive in its “appearance, contents, substance, internal patterns, or other … characteristics,” that singularity alone will enable it to pass the authenticity test.

But because electronic evidence (e.g., audit trails, accounting records, or other files) is so easy to alter, judges are often slow to admit digital evidence just because someone claims to recognize it in court. Has it really been changed in no minute but relevant detail? Someday it may be possible for agents and security managers to “seal” electronic evidence easily by using a digital signature (thereby making the evidence forever “distinctive” and recognizable by sight). But as long as most computer evidence can still be altered electronically—in dramatic ways or in imperceptible detail—without any sign of erasure, most courts will treat it as “fungible” evidence.

When prosecutors present fungible items to a court, they must be ready to prove that the item of evidence they offer is not a substitute, but the same one the agents seized. Whether working with bags of cocaine, bullet shell casings, or electronic data, prosecutors must authenticate any fungible item through a hand-to-hand record of accountability, called a “chain of custody.”

Indeed, judges may demand that prosecutors who offer digital evidence be ready to establish a complete chain of custody—from the person who found it to the person who produced the printout for trial. Of course, if evidence is found on a system and the data that becomes an exhibit is then immediately printed and initialed, the chain of custody may actually be short and simple. (Even so, an IS manager or systems operator might still be
called as a witness to identify the printout and to verify data integrity.) But unless IS managers and systems operators know these rules and know how to forestall challenges to the exhibit, they should think twice before electronically examining and analyzing evidence. They might inadvertently create problems with the identity or integrity of the evidence that a trained investigator could help avoid. For example, a security analyst might alter the evidence by simply retrieving the file, which changes the file's date.

To prevent an intruder from intentionally or mistakenly altering the evidence, the IS manager should make a backup as soon as possible and store it in a secure place. It should be assumed that, from the moment a hacker is discovered, he or she has complete access to the network. Likewise, it should never be assumed that some segments of the system remain off-limits. For example, system operators have sometimes used E-mail to notify users downstream if they see the hacker launching more attacks. But they may mistakenly assume that E-mail is secure. Some hackers not only have learned of criminal investigations this way but also have let the original system operator know it by retaliating electronically against the system. The best alternative is to use the telephone.

The Investigation

The investigation itself consists of tracking down the intruder and gathering evidence to use in possible litigation. The following paragraphs recommend how to successfully perform these actions.

Tracing the Hacker

If an unknown hacker is attacking a system, the first thing both IS managers and law enforcement agents should do is trace the intruder back to the source. Audit trails provide a good start; the communications carrier may also be able and willing to reconstruct part of the circuit. But a trap-and-trace will probably be necessary to identify the source of the call, as Cliff Stoll did in the case he detailed in *The Cuckoo's Egg*.

The need for speed at this point of an investigation is critical. Fortunately, when agents, prosecutors, and telephone carriers work together, they can often get an emergency trap-and-trace operating in days or even hours. Of course, with the multiplication of local and long-distance telephone carriers, this process sometimes requires getting more trap-and-trace orders in distant jurisdictions to complete the trace. It can even be necessary to go overseas for help, if the trace leads in that direction. Although international traces can be difficult and frustrating, law enforcement agencies are succeeding more often with international traces (in part because of hard work in developing international law enforcement connections) and will work diligently to overcome any difficulties.

Once agents locate the hacker, they will probably put a pen register (also called dialed number recorder) on his or her phone for a short while to identify other victims. During this tracing time, law enforcement authorities may ask whether the network can be left open to the hacker to see what he or she is doing. Or they may ask whether the system can be partitioned in such a way that it restricts the hacker but appears to remain open, so that the hacker does not know he or she has been discovered.

This is, of course, an IS manager's decision. No one can—or would want to—force a victim to stay vulnerable if it is too risky. Regardless of what is decided, system operators and security managers remain in control of their system. Law enforcement agents cannot and will not take over a victim's computers, but they will rely on a manager and his or her staff for technical expertise where needed.
Searching for Evidence

Like doctors, IS and security managers are in the best position to assess, contain, and cure the damage if they have been able to examine the patient. Common sense dictates that they must know what an intruder has done (and may still be doing) in the system to be certain they can keep him out. But several federal laws make this a complex area, and IS and security managers must understand how the law affects the way they can monitor their systems. For purposes of legal analysis, IS and security managers should think about systems information in terms of three broad categories: stored files, electronic and voice mail, and real-time communications.

Stored Files.

The first category is regular stored data files—data bases, graphics, spreadsheets—that are analogous to paper in a file cabinet. There may be all kinds of important evidence in the file cabinet, and the Fourth Amendment to the US Constitution (which prohibits the government from engaging in unreasonable searches and seizures) will apply to law enforcement agents in recovering these data files. In short, the law provides that wherever people have a “reasonable expectation of privacy,” police agencies generally may not search their property without a search warrant or without the owner's consent. There are exceptions, of course, and the rules do not restrict private system operators and security managers from searching and seizing files on the system unless they are acting at the behest of law enforcement. But if agents need to gather evidence from stored user files, they will ask the IS or security manager whether, under these circumstances, a reasonable user would expect privacy for his or her files in the system. They will also ask whether the system operator, as someone who has access to all the material, has authority to consent to releasing the files on behalf of the user.

Naturally, computer networks vary considerably in the privacy they accord to users. Some systems guarantee absolute privacy for authorized users, who rely on those guarantees as if they were keys to a bank safety deposit box. Other networks notify users that system personnel may examine the contents of any material on the system, and they explicitly reserve the right to disclose any evidence of crime to law enforcement. Still others tell their users that they monitor for system maintenance and protection and for unauthorized uses. But many networks do not say anything at all—and leave the situation ambiguous, confusing, and almost guaranteed to cause problems eventually. Thus, the users' expectations may range from complete privacy to none at all.

Law enforcement authorities are not in the business of advising what is the best level of privacy for users on a particular network. Whatever balance an organization strikes with users between privacy and security, their relative rights and responsibilities should be spelled out. The clearer the circumstances under which IS managers can examine and disclose user files, the fairer it is to everyone. And the time to examine all these issues is not in the heat of an investigation, but right now!

Electronic and Voice Mail.

The second legal category consists of electronic mail or voice mail that resides on the server in temporary, intermediate storage, incident to transmission. This does not include all electronic mail—only E-mail waiting on a public-service host to be opened by the recipient (and backups of it while it is in that status). The applicable statute (18 USC § 2701, Stored Electronic Communications) was passed by Congress in large measure to
regulate the relationship between public electronic service providers and their customers to protect subscriber privacy. (It prohibits public services from disclosing to unaddressed third parties, including law enforcement, the contents of unopened E-mail messages, except under certain circumstances. Of course, these circumstances include search warrants and subpoenas, in the appropriate case, as well as consent of a party.) IS managers responsible for E-mail on a public network should spend some time mastering the complexities of this statute.

If the network is private, however, this statute does not prohibit voluntarily giving agents a copy of unopened E-mail. Of course, the general reasonable-expectation-of-privacy analysis described earlier would still apply to this E-mail, as it would apply to all stored files under the Fourth Amendment.

**Real-Time Communications.**

The third legal category of material on a network consists of real-time communications—signals while they are in transit. It does not matter for purposes of this statute whether someone is actually watching the keystrokes on a monitor or just capturing them to a file with a network sniffer or similar program. If a transmission of signs or signals is being grabbed as it goes by, the wiretap statute will apply.

It is important, at the beginning, to understand that the wiretap statute, unlike the Fourth Amendment, does not apply just to searches by law enforcement agents. In fact, the statute makes it illegal for anyone to wiretap anyone, and there are both criminal and civil penalties for violating the law. Therefore, all IS and security managers need to be aware of this law and to learn how it can affect their network security monitoring.

Having set out the basic rule that unauthorized wiretaps are illegal, the statute also describes some exceptions to that rule. One exception, which allows telephone companies to monitor voice communications to protect its service, has recently been extended to allow similar monitoring of electronic communications by the service provider. In addition, network administrators should look to another exception that would allow them to monitor real-time communications: the consent exception.

As with stored materials and undelivered electronic mail, real-time communications may be monitored if one of the parties consents. In regard to authorized users, this kind of monitoring can be made a part of the organization's general statement of the rights, responsibilities, and reasonable expectations of privacy on the network. There is no need to address all three of these legal areas separately unless an organization wants to make the rules different. With unauthorized users, however, the different legal categories become much more important.

Most unauthorized users know perfectly well that they cannot expect privacy in a network. If they have managed to somehow misrepresent, lie, steal, or trick their way into the network, the Fourth Amendment will not grant them any cover from anyone, including law enforcement. Having broken into a “house,” they can expect no privacy there.

But this Fourth Amendment analysis (based on the notion of reasonableness) does not extend to the wiretap statute, which defines its own terms. Indeed, the statute, in saying that no one may illegally wiretap a party to a communication, does not restrict that protection to authorized users. Thus, while it defies common sense, it is possible to argue that no one, including IS and security managers, may monitor a hacker's keystrokes without his or her (or another party's) consent. Out of caution, then, the Department of Justice issued its well-publicized “banner letter.” This policy letter advises government systems to use log-in
screens that clearly state the network's monitoring policy and practices—from which the network may infer the consent of all users.

In short, the federal laws that protect the privacy of electronic data form a complex and interwoven fabric over the various categories of information on a system. Some knowledge of these laws is important for clarifying to all users which data is private and which may be monitored.

Working with Law Enforcement

It is popular to preach in high-tech circles that law enforcement does not know how to investigate and prosecute computer crimes, and that reporting them is a waste of time—or worse. This theory has it that, when it comes to electronic crimes, investigators have only two speeds: high or off. Either they want to take over an entire network for the next year, or they do not understand why there is a problem and the need for help.

Actually, six or eight years ago, the second experience was more common. In his book *The Cuckoo's Egg*, Cliff Stoll described the frustrations of trying to work with a law enforcement system that was not prepared for high-tech crimes. That case and others were wake-up calls for law enforcement, however, and much has changed since then. Several years ago, federal investigators and prosecutors embarked on a long-term effort to learn to prosecute these cases right.

For example, in 1991 the Department of Justice began its Computer Crime Initiative, a wide-ranging program to:

- Assess the computer crime problem.
- Facilitate law enforcement cooperation in multidistrict, multiagency cases.
- Help to train investigators and prosecutors in the specialized legal and technical aspects of computer crime prosecutions.
- Address the unique international problems in these cases.
- Work in the area of legislative reform.

This ambitious agenda is the daily work of the Justice Department's Computer Crime Unit, a group of prosecutors who consult constantly with investigators from many agencies, Assistant United States Attorneys, federal policymakers, state officials, and the private sector, including industry and academia.

Of course, it is true that electronic crime cases are often difficult to investigate and prosecute for many reasons—some legal, some technical, some practical. There is a steep learning curve for the uninitiated, a curve that never really levels out. But federal law enforcement agencies clearly believe that mastering emerging technologies is essential to protect the public in the information age, and the federal interagency cooperation and networking are unusually good. Therefore, although not every agent or prosecutor is an expert, they all have ready access to colleagues who are.

In the same vein, computer crime investigators will rely on a victim's system operator and security manager (as long as they are not suspects in the offense) for technical operations involving that network. Doing an extensive computer crime investigation into a complex network is much like having to do engine repair with the motor running. To the fullest extent possible, agents will respect a company's data and equipment and the time of
its staff. They will not be able to disclose everything about the investigation as it progresses, but they will do all they can to convict the person who injured the organization.

**Conclusion**

Federal agents and prosecutors clearly recognize that as computers and communications systems become more powerful tools for law-abiding people, they are equally available to criminals. It is their responsibility to make sure that the victims of computer crime can find the protection of law enforcement when they need it. These agents and prosecutors should be considered an integral part of a network security plan.

**Author Biographies**

Martha Stansell-Gamm

Martha Stansell-Gamm is a trial attorney with the Computer Crime Unit, General Litigation Section, of the Department of Justice. She has extensive experience in criminal and international law, and she lectures frequently to government and private groups on computer crime issues.

The views expressed in this article are the author's and do not necessarily represent the views of the Department of Justice.