Global Information Assurance Certification Paper

Computer Security and the Law

Jimmy Staggs
12/1/2000

Computer security professionals have to keep up to date with a lot of information, and there are a lot of issues competing for our attention. This makes it easy to overlook laws relating to computer crime, the steps that should be taken to ensure that we aren't liable for any damage incurred, and to ensure that an intruder will be successfully prosecuted. Although the more technical subjects are more interesting to most of us, we should all be aware of the pertinent legal issues so we can effectively secure the systems we're responsible for. I am not any sort of legal expert, nor do I have experience in this area, but in this document I will attempt to summarize the most important steps necessary to make the law one more tool to help us do our job effectively.

To start, we should become familiar with the applicable laws. There are now quite a few laws at the federal level relating to computer crime. I'll go over the basics of the ones most relevant to this discussion: The Federal Communications Privacy Act provides the broad and basic law against accessing, altering, or preventing authorized access to electronically stored data without proper authorization. This should be straightforward to security professionals because it directly coincides with the three pillars of protection and attack: confidentiality, integrity and availability. The Computer Fraud and Abuse Act clarifies the definition of federal computer fraud by establishing two felony offenses. The first deals with crimes involving national defense, foreign relations, and computers used for governmental purposes. The second deals with trafficking passwords with intent to commit fraud. Both apply to federal and interstate computer crimes so as not to infringe on individual states' rights. This brings me to an important point: in addition to these federal laws there are often laws at the state or local level that also apply. We should be aware of these laws for our area as well. The Digital Millennium Copyright Act primarily affects code-crackers and software pirates, but it also includes provisions to limit the liability of service providers in certain situations. 'Service providers' can be loosely defined as ISP's, colleges and universities. However, to qualify for the legal protection they must take certain steps beforehand. These include posting and updating copyright policies on-line, and adopting a policy of terminating the accounts of repeat offenders. It should also be noted that the service provider's knowledge of infringing material is considered when determining their liability protection.

Computer crime is a relatively new area in the legal world. Most of the relevant laws have been passed fairly recently, and there haven't been a lot of cases to set precedent for future cases. For this reason the results of trials involving computer crime are less predictable than other sorts of crime. To maximize the likelihood of a favorable outcome, there are a few things those concerned with computer security should do ahead of time to strengthen their stance in the courtroom.

First of all, we need to know that log files are generally considered hearsay evidence, which is not admissible in court. Log files are the most common way for system administrators to determine who did what and when on a system, so they are invaluable if admitted as evidence. In order to exempt the log files from being classified as hearsay, they need to be generated as a part of normal daily operation, and they need to be credible enough to be used daily as well. This is the reason business records on a computer are often admitted as evidence. There must be no reason to think that the log files were generated under unusual circumstances, or by anyone who isn't trustworthy.

Another step security professionals might overlook if they're not thinking of legal issues is the need for policy banners. Whenever a user logs on to a system they should be warned that unauthorized use is illegal and that they are being monitored. This explicit warning will strengthen the legal case against intruders because their continued use of the system after viewing the warning implies that they acknowledge the security policy and give permission to be monitored. Log in messages aren't a sure way to make all the users of a system aware of security policy though. Depending on the service they are using, or the configuration of their account the message may not be displayed. This is why extra efforts should be made to make security policy available. Post it on-line, distribute it to new users, and make sure to explain the consequences of non-compliance.

One more step we can take to make any legal proceedings go smoothly is to respect users' privacy. Because we define and enforce the security policy, we often have full access to the system and the capability to view the contents of users' actions. The prudent principle to work by is to limit what we know to only those things necessary to implement and enforce the security policy, debug problems, or do our job. I don't say this because of any moral or ethical bias, but because the law attaches responsibility and liability to knowledge of wrongdoing. Conversely, if we do find out about any illegal activity on the network or system we're responsible for securing, it is our legal duty to investigate and report it, or stop the activity ourselves if it violates security policy.

I've covered the most important preparatory steps that should be taken, and now I'll go over what should be done *during* an incident to ensure that the law will work with you, instead of against you. There is a wealth of information available on incident handling; it can be a full time job, especially when collecting evidence is considered. For most of us incident handling is only one of many job responsibilities though, so I'll only cover some of the aspects relevant to this discussion.

Because computer data is so easily modified and so sensitive to damage, it is difficult to preserve the integrity of evidence so it will stand in court. The defense can easily cast doubt on the evidence by looking at when it is collected, who was in charge of it, where it was stored, etcetera. This is why it can be important to be careful with anything considered evidence, and document it's location, timestamp and accessibility. It will always depend on the situation and balancing the need for preserving evidence with the need to keep systems up, but ideally you should disconnect the affected machine from the network entirely. This way you can secure the system and be sure it won't be

modified further. Often though, a more realistic strategy is to copy logs and any other relevant files to read-only media like a CD. Data treated in this manner after a crime will hold much more weight in court than data from a system that was compromised and left in operation.

If you decide to involve the FBI in an incident, there are a few things you can do before calling them to help avoid some obstacles in the investigation. Once the government is involved, they can't legally instruct the victim to take any action. This is why it is important to do any investigation of your own before contacting them, so you can have all the information you need for the initial interview with the FBI. Attackers usually don't attack a system directly from their home, or personal computer. Most often there is a lengthy chain of innocent systems between the attacker and their victim, which helps to hide their trail. In their attempt to trace the actual location of the attacker, the FBI is required to obtain a search warrant for every system they need to examine. There can be legal difficulties doing this, because there is no reason to suspect any criminal activity on the part of the intermediate systems that the attacker went through. To avoid these sorts of complications, you should trace the attacker as far as you can by examining your logs, and asking the administrators of the machines your logs implicate to examine their logs, and so forth. This way you might be able to save the FBI a lot of time, which can be very important in this sort of investigation.

As is true with most other aspects of computer security, you'll be best off if you're prepared with clear policies and plans for potential incidents. I've covered what I consider the most important ideas about legal issues that busy security professionals should be aware of. There is a lot of literature available on this topic; check my references for a pointer to more detailed information. By remaining aware of these types of issues, we will be better equipped to enforce the policy of the systems we secure.

References:

Clark, Franklin - Deliberto, Ken. "Investigating Computer Crime". 1996. CRC Press.

Nemeth, Emi - Snyder, Garth - Seebass, Scott - Hein, Trent. "UNIX System Administration Handbook Third Edition". 2001. Prentice Hall.

Biegel, Stuart. "The Digital Millennium Copyright Act". UCLA Online Institute for CyberSpace Law and Policy. 5 Oct 1999. URL: http://www.gseis.ucla.edu/iclp/dmca1.htm

Lide, Casey. "What Colleges and Universities Need to Know about the Digital Millennium Copyright Act". Cause/Effect Journal. Volume 22 Number 1 1999. URL: http://www.educause.edu/ir/library/html/cem9913.html

Rubinstein, Geoffrey. "Computer Fraud". Jones International. 1999. URL: http://www.digitalcentury.com/encyclo/update/comfraud.html

Rieke, Davin. "Crime and Electronic Evidence: Can the Law Adapt to the Information Age?". Stetson University College of Law. 22 Apr 1999. URL: http://www.law.stetson.edu/fitz/courses/computerlaw/papers/spring99/rieke.htm

Sorum, Craig – Harter, Gary. "Hunting the Wily Hacker". SANS Institute Washington DC Conference. 7 Jul 2000. URL: http://www.sans.org/dc2000/FBI-%20Wily%20Hacker.pdf

McMillan, Jim. "Importance of a Standard Methodology in Computer Forensics". Information Security Reading Room. 2 May 2000. URL: http://www.sans.org/infosecFAQ/methodology.htm

Kuethe, Chris. "What are some acceptable procedures for documentation and detective work that will result in court-admissible evidence?". Intrusion Detection FAQ. URL: http://www.sans.org/newlook/resources/IDFAQ/evidence_preservation.htm