

By Debra Littlejohn Shinder

You hear a lot about computer crime, and you know that good citizens report criminal activities to the proper authorities. But you also know that in practice, the police often don't have the time and manpower to deal with every minor offense. If you're a network administrator, you might not be sure exactly which activities you observe are illegal, which should be reported, and to whom you should report.

In general, computer crime laws in the United States can be divided into two categories: federal offenses and state offenses. If a state statute applies, you can call your local police department or state police agency – but they may or may not have the technical expertise and resources to conduct a proper investigation. The FBI and other federal agencies, on the other hand, may be able to get more done – if the case is important enough for them to get involved. In a few situations, computer-related incidents may even fall under city or county ordinances, in which case only the municipal police or county law enforcement (usually the sheriff's department) would have jurisdiction.

Before reporting any incident to law enforcement, follow your chain of command within the company and ensure that upper management approves. Involving law enforcement can result in significant costs. For example, personnel may be required to take time off to prepare for and appear at trial, equipment may be confiscated as evidence and not returned for long periods, and the company's "inside" information may be subpoenaed by the defense attorneys and exposed to the public through the media before and during the trial.

Companies may also want to consider potential damage to their reputations in the eyes of the public if it becomes news that they've been hacked. However, there may be company policies, industry regulations, or state laws that require you to report certain types of data breaches. It's not a decision that a network administrator or IT security specialist should make alone.

Activities you should not report

Don't report port scanning and similar "nonintrusive" activities.

Although port scanning is often a precursor to intrusion or attack, in most jurisdictions it's not in itself a crime. It's more like walking down a hallway in an apartment building and trying each door to see if it's locked. If you find an unlocked door and go inside, that's criminal trespass – but as long as you don't go in, you haven't committed a crime.

Don't report viruses, Trojans, worms, and spyware – at least, not to law enforcement agencies.

Although malicious software is a huge problem that does a great deal of damage and costs companies millions of dollars, law enforcement agencies generally don't (can't) respond to individual malware reports. While those who release viruses and other malware can be prosecuted under Title 18 of the U.S. Code, prosecutors generally go after only those whose malware is widely distributed and causes a large amount of harm. If you encounter a new variety of malware, check the pages of popular antivirus vendors and report to them if it isn't listed. Remember that the sender of a virus often doesn't even know he/she is sending it. However, if you have evidence that a particular person actually wrote and originally released a piece of malware, you should contact local law enforcement or the FBI computer crime squad.

Activities you may report

You may report intrusions and attacks that bring down the network.

Unauthorized access to a computer network is a crime under the laws of many states. If there is little or no documentable injury or monetary loss, however, you may find that law enforcement agencies simply file a report and don't do much more. Jurisdictional issues and caseload often prevent in-depth investigation of computer crimes that are considered "minor." Thus, you would usually report these types of incidents only under a couple of circumstances: If there are policies, laws, or regulations that require it, if you will be filing an insurance claim related to the incident (you'll probably need a police report to file the claim), or if you anticipate a lawsuit in relation to the incident and want to document that you took action.

Activities you should always report

Report intrusions or attacks on major (large corporate) networks or those that deal with sensitive data.

If sensitive data such as client financial information, medical records, customer credit card information, and social security numbers have been compromised, you should report it to the authorities. This is also true if the company has government/defense contracts or deals with other types of regulated information. The FBI's computer crime squad investigates major network intrusions and network integrity violations. You can report these types of attacks to both federal and local/state authorities and let them sort out the jurisdictional issues.

Report intrusions or attacks that result in large monetary losses.

The amount of monetary loss often determines whether a theft type offense is considered a misdemeanor or felony. Felony offenses will get more attention from law enforcement agencies. If there is a large loss, you will also be more likely to file an insurance claim and to need a police report to back it up.

Report cases of suspected industrial espionage.

If an intruder goes after your company's trade secrets, this is a serious federal offense that will be investigated by the FBI.

Report cases involving child pornography.

This is an offense that is taken very seriously by law enforcement, and if child pornography is discovered on your company computers that was not promptly reported, as network administrator, you may be implicated in a criminal prosecution or held liable in a civil lawsuit, or both.

Report emailed or other digitally transmitted threats.

All states have laws against threatening and harassing communications. Physical threats against individuals, terroristic threats, bomb threats, blackmail, and similar electronic communications should be reported to local police.

Report identity theft.

If a user on your network is the victim of identity theft, report it to local police, the FTC, and credit card companies and credit reporting agencies.

Report Internet fraud to the IFCC and the FTC.

If one of your users is a victim of phishing scams or other fraudulent activities perpetrated by email or the Web, report it to the Internet Fraud Complaint Center (IFCC), which is operated by the FBI in conjunction with the National White Collar Crime Center. The Federal Trade Commission also investigates Internet fraud.

Report investment-related fraud or spam to the SEC.

If you receive spam or fraudulent messages related to investments, report it to the Securities and Exchange Commission (SEC).

Report suspected terrorist activities.

If you suspect that your network is being used for communications between terrorists, report it to your local police agency, the U.S. Department of Homeland Security, or via the FBI's "tips" Web site.

Where to report

- **Local/State Law Enforcement:** Call your local police department, county sheriff's office, or state police agency. (Do not call 9-1-1.) Ask for the agency's high tech crimes unit or, in smaller agencies, the criminal investigation division.
- [FBI Computer Crimes Squad](#) or 202-324-9164
- [FBI Tips site](#)
- [Electronic Crimes Task Forces and Working Groups](#)
- [Internet Crime Complaint Center](#)
- [National White Collar Crime Center \(NW3C\)](#)
- [FTC Identity Theft Web site](#)
- [SEC online fraud reporting form](#)