# Collaring the cybercrook: an investigator's view

## In the information age, the cloak is the network and the dagger is the data packet

DAVID J. ICOVE
*Tennessee Valley Authority*

Almost 50 years ago, when asked why he robbed banks, master thief Willie Sutton answered famously, "Because that's where the money is." Today, the "money" is in electrons coursing through the computers the world depends on. Over half a billion electronic messages traverse the world's networks each week. Millions of dollars change hands with the flip of a byte. Military might is increasingly a matter of information superiority. Whether to hobbyist cracker, commercial spy, or international terrorist, these transactions expose the soft underbelly of the information age. (A *hacker* is wildly inventive in software techniques, but a *cracker* is a hacker who breaks into computers.)

Just last year the U.S. Federal Computer Incident Response Capability (FedCIRC) reported more than 2500 "incidents," defined as "adverse event[s] in a computer system or networks caused by a failure of a security mechanism, or an attempted or threatened breach of these mechanisms." The Federal Bureau of Investigation's National Computer Crimes Squad, Washington, D.C., estimates that less than 15 percent of all computer crimes are even detected, and only 10 percent of those are reported. And, without solidly built investigative techniques, which would contribute to a public perception of safety, the very stability of today's military and commercial institutions—not to mention the cybermarkets that are envisioned for the Internet—is called into question.

### A risky business

Computer crime, broadly put, is damaging someone's interests by means of a computer—stealing computer cycles without having authorized access to the machine; stealing, looking at, or changing the data on that machine; using it to get to other machines (an increasingly common situation in this age of networks), as well as more traditional crimes simply updated: hate e-mail, extortion with threats to computer operations, or, in some cases, even physical theft of machines.

JULIAN HARRISON/GAMMA LIAISON NETWORK

**Kevin Mitnick, at one time the most wanted computer criminal in the United States, is shown being arraigned in Raleigh, N.C., two days after his arrest on 15 February 1995.**

Investigation of Federal crimes is generally the responsibility of either the Federal Bureau of Investigation (FBI) or the Secret Service, depending on whether the crimes are of an economic or military nature; in addition, a plethora of Department of Defense investigative services may come into play when appropriate.

By now, most people are aware of how dependent society is on computers. National security is in many ways in the lap of the machines, so to speak—from information on the positioning of reconnaissance satellites to technical analyses of weapons systems. Similarly, just as common criminals have learned that computers are where the money is, so espionage agents have learned that computers are where the intelligence is. Espionage is becoming more and more a game of computer break-ins, computer-based cryptography, and message-traffic analysis.

The cloak has become the network, and the dagger, the message data packet. In his 1989 *The Cuckoo's Egg*, a widely popular recounting of an espionage case, Clifford Stoll wrote how a 75-cent commercial accounting imbalance in California led him to a West German cracker extracting information from defense computers in more than 10 nations. The information was then sold to the Soviet intelligence agency.

The type of criminal in Stoll's book is not an isolated phenomenon, nor can his skills be classified as "dangerous to military" vs. "dangerous to economic" interests. Consider Kevin Mitnick [see photo], in some ways the most celebrated cracker of them all, for the number and audacity of his crimes and for his personal cat-and-mouse game with a leading security expert. Mitnick was an equal opportunity criminal. First in trouble with the law at age 16, when he was put on probation for stealing a Pacific Bell technical manual, he then went from strength to strength. By 1988, when he was 25, he was arrested by the FBI for breaking into the Digital Equipment Corp. computer network and stealing a pre-release version of its VMS operating


0018-9235/97/$10.00©1997 IEEE

system software; he then stored the software for the time being on a computer at the University of Southern California.

Let out in a supervised release program for his "computer addiction," Mitnick then broke the terms of the release, among other things for listening in on a Pacific Bell security official's voice mail. By 1994, the U.S. Marshals, the FBI, the California Department of Motor Vehicles, several local police departments, and several telecommunications companies were looking for him. But his pride led to his downfall: he broke into the computer of Internet security expert Tsutomu Shimomura, and went on to dog him in what became a personal test of skills. In 1995, after a chase crossing a plethora of computer systems and data links, he was caught. Mitnick is now facing a sentence in excess of 10 years in prison.

For obvious reasons, the government is loathe to release information on its lapses in security, and inferences must be made from the few cases that have come to light. In 1990, for example, attacks were reported at facilities belonging to the U.S. Department of Energy, which among other things manages much of the United States' nuclear weapons research. The intruders were prevented from obtaining classified information, and an investigation was begun at once. Several weeks later the intruders were identified and located outside the United States.

More recently, a wiretap order was used to trace and identify 21-year-old Julio Cesar Ardita of Buenos Aires, who used a Harvard University computer to gain access to the Navy Research Laboratory, NASA's Jet Propulsion Laboratory and Ames Research Center, the Los Alamos National Laboratory, and the Naval Command Control and Ocean Surveillance Center. Consider that Ardita was essentially acting on his own and not backed by the tremendous resources of an enemy country's national computer facilities or by payments from an enemy country's treasury. It is clear that military and government systems are enduringly attractive targets for computer criminals, whatever their motivation.

Attacks directed against economic resources, by the same token, are wide-ranging both in intent and damage. They can range from strategic attacks against the nation—the corruption of the banking system, say—to vandalism and plain old theft, whether of money or corporate information. Individual computer users, international agencies, or corporations from small offices to conglomerates are all possible victims of computer crime.

## Where the money was

Some revealing information on the typology of the crimes has been uncovered by a new study conducted by San Francisco's Computer Security Institute (CSI) in cooperation with the FBI. The "1997 Computer Crime and Security Survey" was aimed at determining the scope of the crime problem, and thereby raising the level of awareness of it among present and potential victims [see To Probe Further, p. 36].

The CSI/FBI survey of 563 organizations of all sizes reinforced what was already suspected—that computer crime is a real and dangerously stealthy threat. Sixty percent of the respondents were able to quantify their total loss due to the crimes, and the figure came to more than US $100 million.

Analysis of the breakdown of the statistics on monetary loss and type of crime is tricky, because not all victim groups were able to report financial losses reliably, nor can their monetary loss be compared with other losses due to criminal acts. Bearing that in mind, the report's summaries are interesting. Of those respondents incurring financial loss, three-quarters reported computer security breaches ranging from fraud (26 respondents and $24 890 000 in losses) and loss of proprietary information (22 respondents, $21 050 000 lost) to telecommunications fraud. The rest of the losses were due to sabotage of data or networks, viruses, unauthorized penetration by insiders and outsiders, and an old crime updated—the stealing of laptop computers.

It has long been assumed that most computer security problems are internal. But only 43 percent of the respondents reported one to five attacks from the inside, whereas 47 percent reported the same numbers for attacks from the outside.

## Classifying the crimes

Computer crimes range from the catastrophic to the merely annoying. A taxonomy commonly adopted for them and of use to investigators groups them in terms of the four classical breaches of security. The first, physical security, covers human access to buildings, equipment, and media. The second, personnel security, involves identification and risk profiling of people within and without an organization.

The third group is the most purely technical of the four: security of communications and data. Finally, the preceding three are shackled if gaps occur in operations security—in the procedures in place that control and manage the security against the preceding areas of attacks, as well as procedures for post-attack recovery.

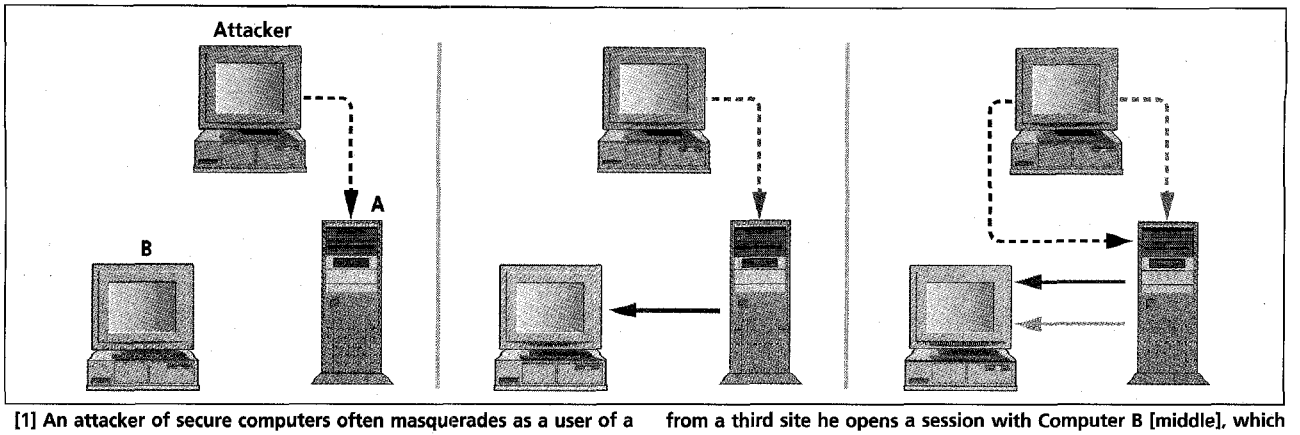
*Physical security* concerns itself with the protection of assets. Breaches of physical security include "dumpster diving," in which offenders physically rummage through garbage cans that may hold operating manuals or specifications. Electronic wiretapping, electronic eavesdropping, and denial or degradation of service also are considered physical crimes, because they involve actual access to the computer or cable.

*Denial of service* covers the physical disabling of equipment or the flooding of communications networks by waves of message traffic. The 1988 Internet Worm, the first Internet criminal event to be reported widely in the public press and the first case prosecuted under the 1986 Computer Fraud and Abuse Act, demonstrated spectacularly the impact of denial of service. This code was released without particular malice in 1988 by its creator, Robert Morris—ironically, as an experiment to enhance security—and was supposed to reproduce itself on one machine after another for a certain time before self-destructing.

But owing to a programming error, like a sorcerer's apprentice the test code continued to multiply on host after host, swamping each in turn until the Internet was basically at a standstill. (In fact, even Morris's e-mailed suggestions for a fix, sent anonymously to system administrators on the first day of the crisis, never made it through the congestion.) Administrators had to shut down computers and network connections, work was halted, electronic mail was lost, and research and other business was delayed. The cost of testing and repairing the affected systems has been estimated at over $100 million. In 1990, Morris was convicted and fined $10 000 (the maximum amount under then-current law), essentially for reckless disregard of the possible damage his code could do, and for using hosts as unwitting guinea pigs—an act of illegal entry no different than any other cracker's.

*Personnel security* aims at keeping people, both inside and outside the company, from deliberately or accidentally getting at computers or systems for illegal purposes. A common example is termed term social engineering, in which the criminal passes herself off as someone authorized to receive from the legitimate user passwords and access rights.

*Breaches in communications and data security* are attacks on the end-user's data and the software managing that data. Data attacks, as defined here, lead to the unauthorized copying of end-user data, whereas attacks on the software managing that data could exploit the so-called trap doors in many programs to hijack a session in progress or insert Trojan horses. Trap doors are supposedly secret patches that programmers put in their code so they can remotely get at it for repair or other actions; Trojan horses, like their Homeric namesake, are programs that seem innocuous but conceal damaging contents. Related to Trojan horses is the "salami attack," in which the attacker repeatedly



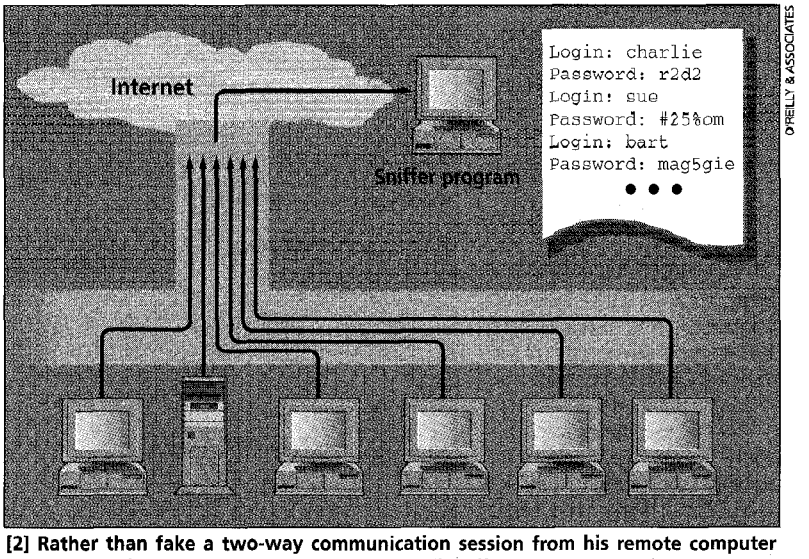

**[1] An attacker of secure computers often masquerades as a user of a machine with high-level access rights. With Internet Protocol (IP) spoofing, the attacker's computer assumes another IP address. The scam has four steps. First, the attacker acquires the IP address of say, an Air Force general's computer [Computer A, left panel], perhaps by the simple scam of social engineering—pretending to be someone to whom that address can be released. Under the guise of that address, from a third site he opens a session with Computer B [middle], which contains classified information. Believing the request to be from A, B sends an acknowledgement and signals it is ready for communication. The attacker completes the deception by again mimicking A, in a final acknowledgment of B's signal [right]. As far as B is concerned, the attacker is the Air Force general, who may act in whatever way his access rights allow.**

slices off and hangs onto a seemingly insignificant round-off on the fractions of pennies in financial transactions.

To put it at its most succinct, taking care of communications and data security is grounded on checking and rechecking a special trinity: the confidentiality, integrity, and availability of data.

*Operations security* contends with attacks on procedures already in place for detecting and preventing computer crimes. A case in point is "data diddling"—small but significant changes in data values, such as adding a few zeros to a $10 checking account. IP spoofing uses a method of electronically masquerading as a pre-existing but idle computer on the network and initiating a session under that assumed, perhaps privileged, identity [Fig. 1].

Password sniffing (obtaining passwords) describes the surreptitious monitoring of users' log-in procedures [Fig. 2]. And then there's scanning, the automatic, brute-force attempt at modem access to a computer by successively changing digits in a telephone number or password (scanners are also sometimes called war or demon dialers).




**[2] Rather than fake a two-way communication session from his remote computer using IP spoofing, an attacker may use password sniffing to try to enter a target computer directly. This mode of attack involves monitoring the first 128 or more bytes of each connection, which sometimes contain users' log-in account names and passwords.**

In both IP spoofing and password sniffing, network traffic is monitored by collecting the first 128 or more bytes of each connection, which sometimes contain both the log-in account name and password.

Two other types of computer crimes, one predominantly personal, the other financial, do not fit well into these categories but are serious and must be mentioned: harassment and software piracy. Harassment by sending repeated threatening electronic messages has become the latest form of hate mail. And software piracy is a staggering international economic problem, costing losses of revenues estimated at $4 billion, according to the Business Software Alliance and Software Publishers Association, both in Washington, D.C.

## Classifying the crackers

Also for the sake of classification and tracking, it is helpful to have a relatively consistent analysis of the types of crackers. One, proposed by convicted cracker (and now security consultant) Bill Landreth, has five categories, each with fairly self-evident occupants: the Novice (mostly quickly bored young kids), the Student (college-age students with an intellectual curiosity in security), the Tourist (who breaks in and persists only if something looks interesting), the Crasher (who delights in simply bringing machines to a halt), and the Thief (the most serious, knowledgeable, and blatantly "criminal" cracker).

For its part, the FBI has established three types of computer criminals: crackers, criminals, and vandals. These so-called offender profiles are based upon interviews of convicted offenders, documented case studies, and scholarly research. (Note that in other contexts these groups are not mutually exclusive: vandalism is legally a criminal act, and so forth.)

*Crackers* are generally young offenders who seek intellectual stimulation from committing computer crimes. Sadly, this type of behavior has often been reinforced as praiseworthy in popular entertainment. In the movie *Terminator 2*, for example, the boy hero is introduced as he electronically steals money from an automatic teller machine, ostensibly to show how smart he is.

Many offenders are juveniles, who view their computers as the next step up from a video game: for example, in 1989 a 14-year-old boy used a home computer to crack the code of an Air Force satellite-positioning system. He reportedly began his cracking career when he was eight years old.

*Criminals*, as a profile class, are often adults subgrouped into those who commit fraud or damage systems and those who undertake espionage. Industrial espionage has long been recognized as a shady competitive tactic. Fraud and damage encompasses all forms of traditional crimes—a fertile field for organized crime.

Banks have always tempted computer criminals. As far back as 1988, a seven-member group hatched a plot against a bank in a large mid-western city. They made use of a wire transfer scheme to siphon off about $70 million belonging to three companies first to a New York bank, and then on to two separate banks in Europe. The transfers were authorized over the telephone, and follow-up calls were made by the bank to verify the requests. But, in the group's fatal error, all the follow-up calls were routed to the residence of one of the suspects.

When the deposits did not turn up, needless to say, the three companies called the bank to find out what had happened. Investigators used the telephone records of the verification calls to trace the crime to the suspects.

*Vandals* usually are not pursuing intellectual stimulation, as when, for example, they deface World Wide Web pages open to the general public. The motivations of electronic vandalism often are rooted in revenge for some real or imagined wrong. A corporation undergoing downsizing should be extremely apprehensive of vengeful vandalism by present or past employees.

## 1. Computer vulnerabilities and countermeasures

| Vulnerabilities | Physical threats | | | |
|---|---|---|---|---|
| | Intruders | Fire | Other sources | Illicit access to data lines |
| Software modifications[a] | | | | |
| Poor audit trail | | | | |
| Ease of illicit access through software | | | | |
| Easily corrupted accessible data | ● | ● | ● | |
| Clear paths for disclosure of information | ● | | | ● |
| Insecure software archives | ● | | | ● |
| Poor configuration control of: | | | | |
| software | | | | |
| hardware | ● | | | |
| communication lines | | | | |
| Poor physical controls | | | | |
| guards | ● | | | |
| environment | | ● | | |
| personnel and management | ● | ● | | |
| Poor contingency planning | | | | |
| Poor communications protection | ● | | | |
| Poor procedures | | | | |
| Susceptible to hazards | | ● | ● | |
| **Countermeasures** | • Alarms<br>• Guards<br>• I.D. badges<br>• Locks on doors | • Smoke/heat detectors<br>• Sprinkler & alarm systems<br>• Area clear of combustible material<br>• "No smoking" rule | • Water sensors<br>• Anti-static carpet<br>• Uninterruptible power supply<br>• Lightning arrestors<br>• Grounding | • Dedicated communication lines<br>• Monitored access points to computers, networks<br>• Shielded computer enclosures |

[a]Includes threats to operating system, applications, and utilities.

One of the better known cases in this category is that of Donald Gene Burleson, a systems security analyst at a Texas insurance company who was upset over being fired. Burleson essentially held his employer's computer system hostage. First, he deleted 168 000 of the company's sales commission records. When backup tapes were used to replace the missing files, he then demanded that he be rehired, or else a "logic bomb" in the computer would go off (this destructive software goes into action when triggered by some computational or externally supplied event, such as certain keystrokes or the date). The "bomb" was programmed to take electronic revenge should the employee be terminated. After his arrest and conviction Burleson was fined $11 800 and sentenced to seven years in prison.

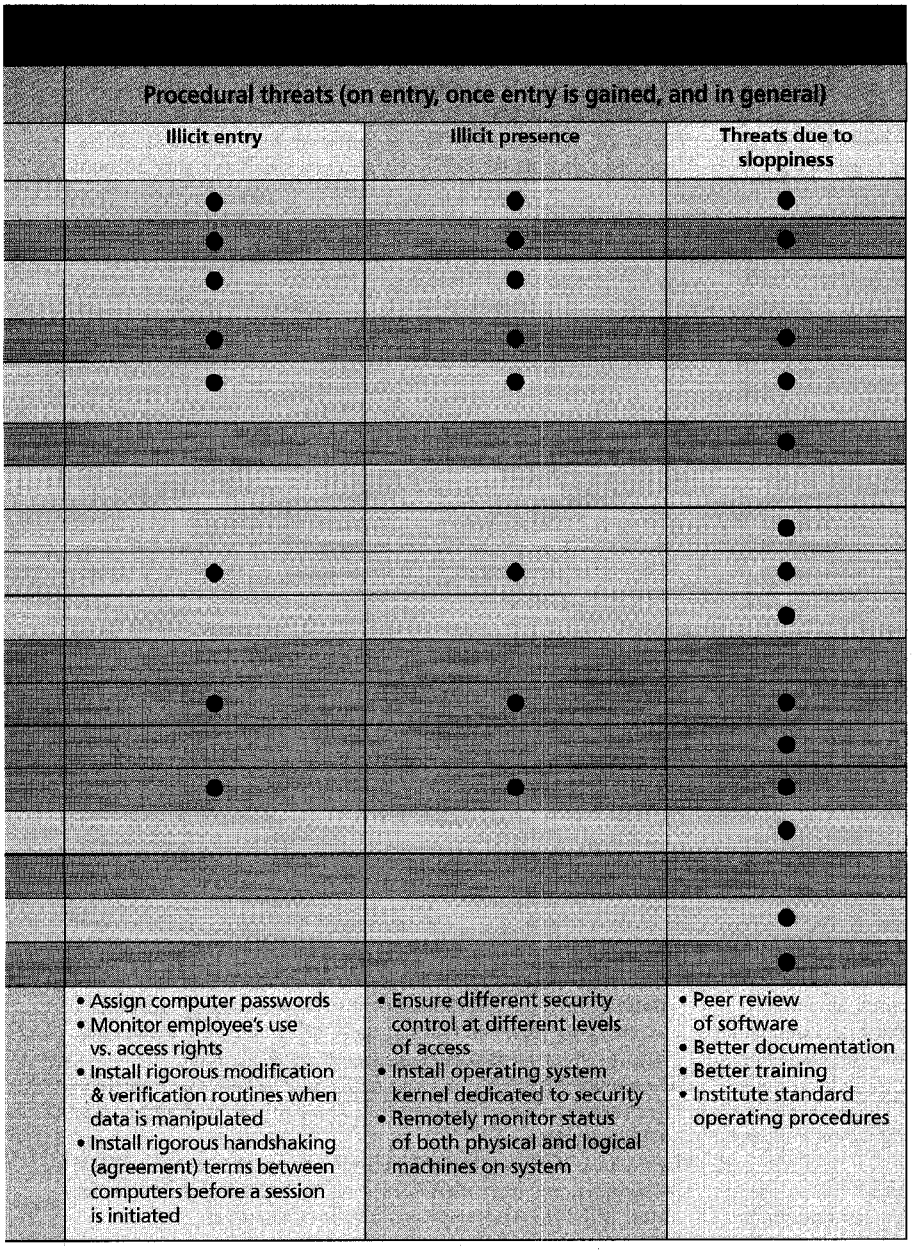
### Computer crime and the law

Prosecuting computer crimes is usually more complex and demanding than prosecuting other types of crimes. The process requires special technical preparation of the investigators and prosecutors and greater dependence on expert witnesses' testimony. Witnesses testifying for the victims may need to explain why the loss of intangibles—proprietary data, for example—are as serious as losses of tangible goods.

In the United States, the most comprehensive computer crime statute to date was included in the Computer Fraud and Abuse Act of 1986, which added six types of computer crimes to Title 18, United States Code, Section 1030. These newly defined illegal activities include those with traditional, Federal impact, such as unauthorized access aimed at obtaining information on national security; access to a computer used by the Federal government; and, interestingly, unauthorized access to a computer that itself is used to access a Federal government computer.

Equally welcome is the strengthening of the legal defense against economic crimes. Federal law now covers unauthorized interstate or foreign access with intent to defraud or obtain protected financial or credit information; unauthorized access that causes $1000 or more in damage; and fraudulent trafficking in passwords affecting interstate commerce.

Another Federal statute, the Electronic Communications Privacy Act of 1986, is intended to provide security for electronic mail on a par with what users would expect from the U.S. Postal




Service. As with postal letters on land, it is now a felony to read other people's electronic mail without their permission.

Precisely how does this affect me, you may be wondering. In brief, should your organization, whether public or private, fall victim to a computer crime, it should immediately seek competent legal representation. You may need to pursue legal remedies to what on the surface first appears to be a nuisance offense.

In their *Practical Unix & Internet Security*, Simson Garfinkel and Gene Spafford [see To Probe Further, p. 36] detail the following potential legal scenarios, which often lead to messy results:

- Unauthorized access to classified or sensitive data may require mandatory notification to investigator agencies.
- Being aware of criminal activities without reporting them may make you liable for your inaction.
- Deciding as an executive officer of a company not to make a report and cooperate with law enforcement may lead to your shareholders suing you.
- After filing an insurance claim for damages resulting from computer intrusions, you may be required by the insurance company to pursue legal action against the suspected intruders.

In sum, reporting suspected computer intrusions to the appropriate officials, combined with immediately obtaining competent legal guidance, will substantially reduce your liabilities and increase the likelihood of success by law enforcement in dealing with computer crime.

The prime contact to make after any computer incident is the 24-hour CERT (Computer Emergency Response Team) Coordination Center, which was formed by the U.S. Defense Advanced Research Projects Agency (Darpa) in November 1988 after the Internet Worm disaster. A similar, but private, organization is the Forum of Incidence and Response Security Teams (First), founded in 1993 [for contact information, see To Probe Further, p. 36]. Understanding the computer crime laws is also key to establishing good internal policies for computer crime prevention.

## What the offenders teach us

In the late 1980s, the U.S. government started a series of studies designed to better understand the motivations, tools, and techniques of computer criminals. The information most sought after was good motive-based offender profiles, as well as a command of the lessons learned from criminal events, information which could be relayed to the computer security and law enforcement communities. In the end, the FBI prepared a detailed chart of the vulnerabilities of computer systems, possible threats to them, and countermeasures to take against the threats [see a summary of the chart, left].

Consider a member of a cracker group thought responsible for charging more than $30 000 in unauthorized telephone calls through voice mail systems as well as breaking into credit bureau computers to obtain financial information. This individual pleaded no contest to the charges, was sentenced to provide 150 hours of community service, and given a fine of $255 and court costs. The youthful offender was convicted as an adult.

Time and again the offender had accessed credit bureaus and had been quite successful in the art of social engineering, that is, misrepresenting himself as an authorized user or official; he had an outspoken hatred for law enforcement in general; and, when questioned, he had told police only what he believed they already knew.

Further study of the circumstances of the case and the offender's behavior turned up several lessons in security, as well. He had easily gained access to computer systems using default accounts, often even invading the root directory, from which all system-wide administrative procedures can be implemented. He had carefully located known weaknesses in computer systems and had been undeterred by warning calls from security personnel.

## Preventive weapons

In the fight against unauthorized access from external sources, or attempts from inside by personnel to exceed their authorized access levels, three distinct computer-crime prevention tools have emerged: firewalls, auditing, and risk assessments.

Firewalls are software programs specifically designed as a

security interface between the Internet and a local host. When correctly installed and maintained, they safeguard against unauthorized access from the Internet, and can control access from within a company network to the Internet. Usually placed upon a secure workstation dedicated only to hosting security software, most firewalls use Unix as their native operating system. An effective firewall also has mandatory file and virus checking to reduce the likelihood of importing malicious computer worms or code.

Auditing data transactions with logs—keeping track of who accesses what and with which processes—is a natural byproduct of a firewall. In addition to providing security, this data record can reveal historical patterns in both internal and external attempts to break into computer systems and data. A critically important security job is timely reviews of the log and user activity, by both trusted human administrators and automatic procedures that take action upon evidence of anomalies.

Risk analysis—establishing a plan for the security and privacy of each computer system—balances the cost of various types of protection against the costs of doing without them. Periodic risk assessment is the best pro-active weapon against computer crimes. Indeed, Section 6 of the Computer Security Act of 1987 (Public Law 100-235) mandates that U.S. Government computer systems containing sensitive information undergo approved risk analyses. [Note: firewalls, auditing, and risk assessments will be discussed in detail in coming issues of *Spectrum*.]

## For whom the bell tolls

Computer crime is a grave problem. It threatens national security with opportunities for modern criminals that go far beyond anything previously experienced. Although improvements in security are helping to keep it under control, the criminals are keeping pace with technology.

Surveys, case studies, and observations suggest that major problems will be encountered before the year 2000. Networks will continue to be vulnerable, and financial, medical, and credit reporting networks will endure major outages as a result. Political extremists and terrorists targeting critical services will score successes, as will organized crime. Major international high-technology financial thefts involving electronic fund transfers and "Internet commerce" will take place. To top it all off, court-qualified investigators and laboratory evidence technicians will be in short supply.

But let me put all this as personally as possible. If you are a manager or owner of a business, computer crime can undermine everything you have worked so hard to accomplish within your organization. Computer criminals, masquerading as authorized users, may be able to figure out how to access and steal the business plans you've labored over. Trade secrets about the product on the verge of being released may help a competitor beat you to market. Disclosure of confidential material may also lead to a loss of credibility with your vendors and put your company at risk of not receiving government contracts.

If you are involved in law enforcement, whether as an investigator or a prosecutor, you may have to deal with either a computer crime investigation or a case where computers have been used by those responsible for other crimes. You may have to assist in the preparation of a subpoena for computer crime evidence, participate in the collection of computers and computer media during an arrest or during the execution of a search warrant, or be called upon to conduct a major investigation of a computer crime.

As the victim of a computer crime, you may be asked by law enforcement to assist in tracking a computer trespasser, or in putting together data that will later serve as evidence in the investigation and prosecution of a suspected computer criminal.

If you are an ordinary computer user, realize that you, too, are vulnerable. If you fail to protect your log-in account password, files, disks, and tapes, and other computer equipment and data, they might be subject to attack. Even if what you have is not confidential in any way, having to reconstruct what has been lost could cost hours, days, or longer in productivity and annoyance.

Finally, in this era of networked computers, even if your own data is not a worry, you have a responsibility to protect others. Someone who breaks into your account could use that account to become a privileged user at your site. If you are connected to other machines, the intruder could then use your system's networking facilities to connect to other machines that may contain even more vulnerable information.

The word *responsibility*, at all levels, sums it up. By working together responsibly, far more often than not the good guys can outmatch their adversaries. ◆

## To probe further

More detailed techniques and case studies can be found in *Computer Crime: A Crimefighter's Handbook* (O'Reilly & Associates, Cambridge, Mass., 1995), by the author of this article, Karl Seger, and William VonStorch, and in the FBI manual, by the same three authors, on which the book was based: *The Prevention and Investigation of Computer Crime: A Training Manual* (The Federal Bureau of Investigation, 1995).

Kenneth Rosenblatt's *High Technology Crime: Investigating Cases Involving Computers* (KSK Publications, San Jose, Calif., 1995) is also excellent for security personnel. It comes with a disk containing software for search tool kits and sample search warrants.

A good mix of technical and practical knowledge is presented in *Practical Unix & Internet Security*, by Simson Garfinkel and Gene Spafford (O'Reilly & Associates, Cambridge, Mass., 1996).

The most recent survey of the effects of computer crime, and which was highlighted in this article, is discussed in Richard Power's "Computer Security Issues and Trends" (Computer Security Institute, San Francisco, Vol. 3, Spring 1997).

For obvious reasons, the computer security community on the Internet is vast. One well-organized list of resources is at the Library of Congress's Web site, http://lcweb.loc.gov/global/internet/security.html. Another is that of the Coast (Computer operations, audit, and security technology) lab at Purdue University: http://www.cs.purdue.edu/homes/spaf/hotlists/csec.html.

For information explicitly on investigation see the Web site of the High Technology Crime Investigation Association, http://htcia.org/HTCIA_CH.html.

The 24-hour hotline of the Computer Emergency Response Team Coordination Center (Cert/CC) is 412-268-7090; fax, 412-268-6989; Web, http://www.cert.org; ftp, ftp://info.cert.org/pub/.

Clifford Stoll's *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (1989; reprint, Pocket Books, New York, 1995) first stirred public discussion of the more subtle byways of computer crime.

Good starting points from which to look at security from the cracker's perspective are http://www.digicrime.com and http://www.2600.com, the home site of 2600 Magazine. A large collection of links to sites of interest to crackers is http://www.ica.net/pages/srusso/hack/wwwlinks.html.

## About the author

David J. Icove (M) is manager, special projects and technical investigations, U.S. Tennessee Valley Authority Police. Prior to joining the authority in 1993, he served nine years as an instructor in the Federal Bureau of Investigation's Behavioral Science Unit, Quantico, Va., where he profiled computer crime and bombing cases. A co-author of several textbooks on law enforcement and security-related topics, Icove holds degrees in electrical engineering and a Ph.D. in engineering science from the University of Tennessee, Knoxville, where he is an adjunct professor of electrical engineering. He is a registered professional engineer.

*Spectrum* editor: Robert Braham