Chapter 1

Spies

"I could have been a devastating spy, I think, but I didn't want to be a devastating spy. I wanted to get a little money and to get out of it."

—Robert Hanssen, FBI agent and convicted Soviet spy

Getting to Know Spies

Computer spies typically don't wear trench coats. They don't dress in tight black clothes and hang upside down from trapeze wires over your keyboard. They probably aren't named Boris and don't speak with heavy Slavic accents. Most of them aren't even hackers or crackers, and likely wouldn't know the difference between a rootkit and root beer. If computer spies don't match the popular media's perceptions, just who are they?

As with most avocations, computer espionage is divided into the amateurs and the professionals.

Amateurs are casual spies. Although they may have very good reasons for snooping, their livelihood doesn't depend on it. These spies have a bit more experience with computers than the average user. That doesn't mean they're extremely technical; it means only that they have taken the time to learn about various technologies that can be used for computer eavesdropping and then applied that knowledge for espionage purposes. Learning about spying tools and then acquiring them is only a point and click away with an Internet connection. When you think about these types of spies, don't picture Tom Cruise or Sandra Bullock. Instead think of your boss, coworker, spouse, children, or the neighbor next door.

Professional spies tend to have more technical experience than the amateurs. One aspect or another of the professionals' jobs is to spy on people. This spying can be legal, as in the case of a law enforcement officer collecting intelligence for a child pornography criminal case, or illegal, in the case of a spy hired to obtain trade secrets from a corporation's network. Although these spies use some of the same tools and technologies that the amateurs use, they have a deeper understanding of the technology as well as access to more advanced and sophisticated eavesdropping tools. As with amateurs, you usually can't tell a professional spy by his or her appearance. Consider Aldrich Ames or Robert Hanssen: white, middle-class, average-looking CIA and FBI insiders who successfully spied for the Russians but blended in with society for years. Again, professional computer spies don't match the popular media's romanticized versions of espionage reality—although perhaps one or two might have a partner in crime named Natasha.

There are two reasons why it's important to have insights into the different types of spies:

- ✓ **To understand the technical capabilities and limitations of a potential adversary.** This is obvious because you want to make sure that your own security measures can withstand a spy's attempt to breach them.
- ✓ **So you can put yourself in the spy's shoes.** Throughout this book, there are sections that present spying tactics, specifically regarding how people spy on computers. In most of these sections, you're asked to put on the spy's trench coat so you can better assess your own security; to fully protect yourself, however, you need to know not only the tools and the techniques, but also the mindset of a spy. Popular culture has the saying, "What would _______ (Jesus, Gandhi; fill in your favorite wise role model) do?" When you review your security, you need to ask, "What would Corporate Spy (or whichever type of spy may be a threat) do?"

The famous Chinese military strategist Sun Tzu said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Throughout this chapter, the concepts of knowing the enemy, knowing yourself, and knowing both the enemy and yourself are applied to computer spying.

What Spies Are After and Who They Are

Let's start with knowing the enemy. Computer espionage is about the purposeful discovery of information or evidence. If you use a dictionary definition (in this case, the *American Heritage Dictionary of the English Language, Fourth Edition*), information is "knowledge of specific events or situations that has been gathered or received by communication, intelligence, or news." Evidence, on the other hand, is "a thing or things helpful in forming a conclusion or judgment." An industrial spy may be looking for secret information on a Microsoft project manager's laptop that specifically relates to the company's future and hush-hush Longhorn operating system. A wife who suspects her husband of having an online affair may be looking for evidence in e-mail messages in an attempt to confirm her suspicions. Depending on what the information is, it could evolve into evidence. For example, a phone number stored in a PDA address book could belong to a known drug dealer and become supporting evidence for a criminal case.

Remember that spying is a purposeful activity. Although the suspicious wife may have stumbled across evidence that her husband was cheating because he accidentally left an Instant Messenger window open on the family computer, that's not spying. She wasn't actively seeking the information.

The types of information and evidence gathered can be very targeted or generalized, depending on what the spy is trying to accomplish. Perhaps he is looking only for financial information that relates to an upcoming merger and will be content with snooping through spreadsheet files with accounting information. On the other hand, a government intelligence agency may examine the entire contents of a hard drive that belonged to a terrorist, seeking not only evidence, but any information that may relate to future terrorist attacks.

In addition to information and evidence, there are two other important concepts in computer espionage: The activity is typically unauthorized and unknown. In most cases, you aren't going to give explicit or implicit permission to have someone snoop through your computer. Exceptions might be in the workplace in which employee monitoring takes place or when you tell the friendly police officer that you don't have anything to hide, you don't need a lawyer, and certainly he can look at your computer. Also in some types of law enforcement investigations you won't have a say if a court has granted permission to a police agency to spy on your computer because of suspected illegal activities on your part. Remember that *unauthorized* doesn't necessarily mean *illegal*. Although breaking into a computer network to steal trade secrets clearly violates a number of laws, placing a keylogger on your son's computer without his permission to see if he talks to his friends about doing drugs would not be illegal, though it may be unethical to some people.

The second element of computer spying is that if you're the target, you don't know it's taking place until perhaps after the fact. Unlike clothing manufacturers, eavesdroppers don't go around leaving tags on computers that read "Snooped on by Spy #39." Sometimes, spies do leave tracks, but they usually aren't that obvious. Whoever is spying doesn't want you to know they are looking for information or evidence. Exceptions would be a publicized employee-monitoring program or the government's ECHELON data surveillance system (discussed later in this chapter), which is known about — much to the chagrin of those running the program.

x-ref

ECHELON is an example of the government's frequent "cult of secrecy" attitude. Although the existence of ECHELON has been exposed, the government steadfastly refuses to acknowledge its existence. For more on ECHELON and other data surveillance systems, turn to Chapter 13.

So far, this discussion has all been about what spies are generally after, but we still haven't answered Sun Tzu's question of knowing who the enemy is. This is important because it gives us insights into their motivations and methods. Thinking like the bad guys is a valuable exercise in helping you protect yourself from them.

In general, spies can be lumped into seven different categories:

- ✓ Business spies
- ✓ Bosses
- ✓ Cops
- ✓ Private eyes and consultants
- ✓ Spooks
- ✓ Criminals
- ✓ Whistleblowers
- ✓ Friends and family

Let's take a quick look into the world of each type of these spies to better understand who they are and what they are after.

Business Spies — Economic Espionage

Economic espionage is a large, yet often ignored problem. Trade publications and organizations and the news media have been warning businesses about the dangers of economic espionage, formerly called industrial espionage, since the 1980s. The warnings seem to have fallen on deaf ears.

Consider these key points of a study released in 2002 by the American Society for Industrial Security, U.S. Chamber of Commerce, and PricewaterhouseCoopers, a survey of Fortune 1000 corporations and 600 small to mid-sized U.S. companies:

- ✓ Forty percent of the companies that responded to the survey reported having episodes of known or suspected loss of proprietary data. (Cutting away the jargon, that means someone on the inside or outside spied on them and stole company information.)
- ✓ Proprietary information and intellectual property losses accounted for between $53 billion and $59 billion.
- ✓ Economic spies are looking for information; they most commonly target research and development, customer lists and related data, and financial data.
- ✓ Despite the potential impact of possibly successful attacks, only 55 percent of the responding companies said their management was concerned about information loss and were taking precautions to prevent it. The implication of this is a significant number of managers underestimate or don't understand the risks and costs of data theft.

Companies suffering economic espionage attacks don't just suffer simple financial losses. They also have to contend with eroded competitive advantages, legal fees in the case of litigation, and diminished stockholder and public trust if an attack is publicized (which many are not publicizing for this reason alone).

Business spying isn't confined just to large corporations, either. Smaller companies, from mom-and-pop retailers to light manufacturers that operate at thinner margins without the cash reserves of a larger corporation, may actually suffer more significant damage from economic espionage.

Former employees, domestic and foreign competitors, and on-site contractors are the usual perpetrators of economic spying. (It's worth noting that economic espionage is very different from competitive intelligence. Competitive or business intelligence is practiced by using legal and open source methods. Economic espionage is where illegal means are used to obtain information. Granted, at times there can be gray areas, but most business intelligence professionals adhere to a fairly strict set of ethics.)

x-ref

For more information on the differences between legitimate competitive intelligence and illegal espionage, visit the Society of Competitive Intelligence Professionals Web site at `www.scip.org`.

Although movies and TV shows portray corporate spies as shadowy mercenaries who cleverly break into super-secure locations, the reality is that insiders who have access to unsecured information are responsible for most economic espionage. Current or former employees with greed or revenge as motivation are much more of a threat than professional spies hired by a competitor.

Spies: Niku versus Business Engine

In August of 2002, several dozen FBI agents raided the offices of Business Engine, a Silicon Valley software company specializing in Web-based collaboration tools. The raid was prompted when competitor Niku Corporation discovered in its server logs that someone with an IP address that mapped back to Business Engine had used Niku passwords to access the company's network more than 6,000 times. More than 1,000 documents had been downloaded during the intrusions, including information about upcoming features, lists of potential customers, pricing, and sales call schedules. Subsequent investigations revealed that since October 2001, outsiders had logged onto the internal Niku network, using up to 15 different accounts and passwords to access proprietary documents.

As of late September 2002, the once-thriving Niku was on the brink of being delisted by NASDAQ because of its low stock value. It doesn't take a Harvard MBA to speculate that an extensive economic espionage campaign could have contributed to Niku's ill fortunes.

Niku has filed suit against Business Engine, and it will be interesting to watch the details of this case emerge.

The problem isn't confined only to lower-level employees. Jose Ignacio Lopez, the head of purchasing for General Motors, abruptly resigned in 1993 and took a job with Volkswagen. GM later accused Lopez of masterminding the theft of more than 20 boxes of research, sales, and marketing documents. Included were blueprints for an assembly plant GM hoped would displace VW's dominance in emerging small-car markets. In 1997, the case ended when VW admitted no wrongdoing, but settled the civil suit by paying GM $100 million and offering to buy $1 billion of GM parts over the next seven years. German prosecutors eventually dropped industrial espionage charges against Lopez, but ordered him to donate a quarter of a million dollars to charity.

Outsider attacks still occur though, and are either committed by an employee or agent of a competitor. Outside attacks typically fall into two categories:

- ✓ **Opportunistic attack.** A competitor may casually see if information may be easily accessible, akin to twisting a doorknob to see whether it's locked. Information is stolen if there's not much of a risk of discovery or involves little effort. An example of this attack is a spy using a port scanner or vulnerability-assessment tool to see if there are any holes he can exploit to enter a corporate network. If exploitable vulnerabilities are discovered, a targeted attack may be launched.
- ✓ **Targeted attack.** A targeted attack is a serious attempt to steal information. The spy has a specific goal and employs a variety of techniques to get what he wants. When the monetary stakes are high, a large amount of money and resources may be committed to a spying operation.

Because computers are used to store all sorts of corporate information, they present a prime target for business spies. Networks, laptops, desktop PCs, and PDAs are all vulnerable to attack.

The technical skills that business spies have range from eavesdroppers with minimal skills, such as copying a confidential file to a floppy disk, to skilled technicians who can easily bypass a firewall to access a corporate database.

x-ref

There are strict penalties for economic espionage in the United States. Turn to Chapter 2 for details.

Bosses — Employee Monitoring

Employee monitoring in the United States is growing rapidly. In the American Management Association's (AMA) 2001 survey on Workplace Monitoring & Surveillance, 77.7 percent of major U.S. companies stated that they recorded and reviewed employee on-the-job communications and activities. This amount is double what the AMA reported in its first monitoring report released in 1997.

If you work for someone else, there's a good chance the boss is spying on you. That means your e-mail, Web surfing, instant messaging, and hard drives could all be under scrutiny. Employee privacy really doesn't contribute to the bottom line and in fact may detract from it. Employers are interested in finding evidence that you aren't being productive or are somehow violating company policy.

How can companies get away with this?

When you're dealing with a government entity, you have a series of constitutional rights that protect your privacy. When it comes to private businesses and the workplace, however, these rights don't apply. Because your time is being paid for by an employer and the computer equipment you're using belongs to the company, you shouldn't have any expectation of privacy when it comes to your computer activities.

Anytime an employer has a compelling interest in what you do at work because of legal, productivity, performance, or security reasons, he or she can monitor your computer, as well as your telephone, coffee breaks, and just about anything else short of using the company restrooms.

Monitoring is either accomplished at the server, where administrators can view logs or examine exchanged electronic messages, or at the desktop PC, where keyboard-monitoring software can be installed.

x-ref

Keyloggers are discussed in detail in Chapter 8.

Typically, the corporate IT staff or an outside consultant is responsible for implementing the monitoring program and will be fairly technically skilled. Consider that if you try to defeat an employee-monitoring program, you might end up calling attention to yourself and presenting a personal challenge to a bored system administrator to see what you're up to.

Spies: Justified Snooping

Employee monitoring, whether by using video cameras, recording phone calls, or monitoring computers, is big in corporate America.

A driving factor for this is that a number of local, state, and federal court decisions have ruled that employers are responsible for employee wrongdoing while they are at work. Companies use this as one rationale for implementing employee-monitoring programs. Employers can also justify workplace monitoring as part of reducing legal liability.

There have been a number of high-profile monitoring cases. In 1995, a subsidiary of Chevron was sued for sexual harassment over an e-mail that circulated through the company entitled "25 Reasons Why Beer Is Better Than Women." The case was settled out of court for $2.2 million, and Chevron now monitors employee e-mail. In July 2000, Dow Chemical fired 50 employees and disciplined 200 others for accessing online pornography. In October 1999, 40 employees at Xerox were fired for surfing forbidden Web sites (Xerox monitors Web usage of all of its more than 90,000 employees worldwide).

Whether employees like it or not, employee monitoring has become a commonly used management tool.

Despite the rather Orwellian overtones of employee monitoring, most responsible companies will at least be upfront about it. Monitoring programs should be publicized in employee handbooks, employment agreements, and computer banners. Letting employees know that a monitoring program is in place in most cases is a better deterrent against bad behavior than being sneaky.

The coming years will likely bring legislation at the state level that increases workplace privacy, but for now it's important to realize that while at work, your electronic on-the-job privacy can be invaded at your employer's discretion. While there are countermeasures you can take against snooping bosses, the best option is to simply keep your personal life separate from the computer activities of your day job.

Cops — Law Enforcement Investigations

Aside from employee monitoring, another form of legitimate spying is performed by law enforcement. While most cops would never consider themselves spies or think they'd be involved in espionage, it's all a matter of semantics. Intelligence activities, surveillance, and investigations are all much more socially acceptable terms for spying.

Cops are primarily interested in finding evidence that you've committed some crime. From a computer standpoint, evidence may be collected before or after you've been charged with the crime.

If you're under investigation, your network activity might be monitored (including e-mail, instant messaging, and Web browsing), and under certain circumstances, officers might gain physical access to your computer to look at its contents or place monitoring hardware or software on it.

If you've been charged with a crime, almost certainly your computer will be seized and will undergo forensic examination. In this examination, a technician searches through your hard drive and any other storage media to find any evidence that may relate to this specific crime or possibly other crimes.

x-ref

Computer forensics, the process of gathering evidence from computers, is discussed at length in Chapter 5.

When it comes to computer spying, police officers need to follow a very strict set of rules and guidelines. The Constitution gives citizens a number of rights that protect them from unreasonable government intrusion, whether they are criminals or not. For law enforcement investigations, this protection requires getting a court order or search warrant from a judge before the computer surveillance activities can begin.

Following the terrorist attacks of September 11, 2001, however, Congress has recently granted broader investigative powers to law enforcement agencies.

x-ref

Expanded powers under the USA Patriot Act (USAPA) as they relate to computer spying are discussed in Chapter 2.

Despite having to follow strict legal rules for evidence collection, individual law enforcement officers have abused their power in the past, whether by design or accident, and stepped outside the law. An example is a secret internal FBI memo that was leaked in October 2002 that described "mistakes," such as intercepting innocent citizen's e-mail, recording the wrong phone conversations, illegally videotaping suspects, and performing unauthorized searches. Although most of the time law enforcement agencies abide by set rules of engagement, don't be surprised if sometimes they don't.

How competent a cop will be at computer spying varies tremendously. Generally, law enforcement is completely understaffed when it comes to technicians who have the skills and knowledge to effectively collect and analyze electronic evidence. Most cops aren't that savvy when it comes to computers, and the minority that are savvy are overburdened with large caseloads where electronic evidence is involved. Police agencies tend to hire from within and then send officers outside to get the training they need to perform their new job duties. Because of higher-paying positions in private industry and the differences in police and high-tech culture, very few skilled computer industry people who would be excellent at evidence gathering are attracted to law enforcement.

As a general rule of thumb, the larger the police agency, the greater the chance of having a technical specialist available to deal with computers. Federal law enforcement agencies such as the FBI and Secret Service have the most highly trained personnel, but again, their skills vary on an individual basis.

Busted: Good Cop, Bad Cop?

During the summer of 2000, the FBI was investigating a series of e-commerce site computer break-ins in which credit card information was being stolen. The trail pointed to crackers in Russia.

FBI Special Agent Michael Schuler had a good idea who the suspects were and designed an elaborate sting operation to catch the perpetrators. In November 2000, Vasily Gorshkov and Alexey Ivanov came to the United States to interview for jobs with a Seattle computer security company called Invita. Invita employees asked the pair to demonstrate their skills. In the process, they logged on to their own computers in Chelyabinsk, Russia. Instead of getting stock options, the two Russians found themselves in the stockade. Invita was a fake company set up by the FBI, and the interviewers were all FBI agents.

Gorshkov and Ivanov didn't know it, but the FBI had installed a sniffer on the computer they used to access the computers in Russia. Immediately after they were arrested, Schuler used the sniffed accounts and passwords to log on to the suspect's computers and download 250GB of evidence that would link the two men to the computer break-ins and credit card fraud.

Schuler received accolades for being the first FBI agent to electronically "utilize the technique of extra-territorial seizure." However, no search warrant was ever issued before the data was downloaded (one was issued after the fact), and no one from the FBI ever talked to Russian law enforcement. Gorshkov's attorney argued these points and the fact that Russian laws had been violated, but the judge ruled that Russian law did not apply to the agents' actions.

Nearly two years later, in August 2002, the FSB, Russia's Federal Security Service, accused Schuler of unauthorized access to computers in Russia and began criminal proceedings against him. The issue will likely be resolved diplomatically, but Schuler probably won't be planning any vacations to Eastern Europe in the near future.

As a postscript, Gorshkov was sentenced in October of 2002 to three years in prison and ordered to pay restitution of $690,000. Ivanov pleaded guilty to a number of charges in August 2002. As of mid-March 2003, he has yet to be sentenced.

Private Eyes and Consultants — Private Investigations

Other types of spies, who may be legally or illegally electronically eavesdropping on you, are private investigators and technical consultants. These specialists find evidence that relates to criminal or civil matters, and it may be used by businesses, law enforcement, or individuals. Private eyes have formal investigative backgrounds, usually gained from dealing with a variety of different types of cases. Consultants tend to have specific technical areas of specialization, particularly in computer networks and forensics.

PRIVATE EYES

Although the stereotype of Sam Spade gumshoes in trench coats is etched into American culture, private eyes have changed with the times and are increasingly engaging in computer-related investigations.

Private eyes have long been involved in audio and video surveillance activities, and it's a natural progression for them to start becoming involved in computer surveillance. Traditional private investigators often come from law enforcement and likely have limited computer skills. Generally, the average private investigator has some technical computer skills but will likely employ easy-to-use and common spying tools. However, a new generation of PIs that have grown up around computers will be much more skilled than their fathers and grandfathers.

Spies: Garbage Gate

In 2000, database giant Oracle hired detectives from Investigative Group International (IGI) to investigate and research two organizations: the Independent Institute and the Association for Competitive Technology (ACT). (IGI is staffed with a number of former FBI agents and gained some notoriety for being retained by President Bill Clinton to investigate matters related to Paula Jones and Monica Lewinsky.) This happened while the Microsoft antitrust investigation was underway, and both the nonprofit organizations, which were strong supporters of Microsoft, were reputed to have financial ties to the Redmond, Washington company.

During the summer, a woman identifying herself as private investigator Blanca Lopez offered janitors $700 in cash to go through ACT's office trash. Lopez had gained access to the locked building by using a cardkey that belonged to Robert Waters, a private investigator associated with IGI, who had rented an office in the same executive suite as ACT under the name of Upstream Technologies.

When the story broke, Washington D.C. police said there was no Blanca Lopez registered as a private investigator in the city. Investigative journalists questioned whether Upstream was a front company, whose only purpose was to provide a cover for being in the same building as ACT. Larry Elison, Oracle CEO, admitted hiring IGI, justifying that it was important to expose Microsoft, but he carefully sidestepped the trash issue stating, "I'm prepared to ship our garbage to Redmond, and they can go through it."

Basically what appears to have happened was Oracle believed ACT and the Independent Institute, both promoting themselves as independent advocacy groups, were actually front organizations for Microsoft, charged with influencing public opinion to favor Microsoft during its antitrust trial. Someone tipped off the *Wall Street Journal* after the cash-for-trash incident, and journalists there were able to piece together the Oracle and IGI relationship. Oracle maintained that IGI informed the company that they would only use 100-percent legal investigative techniques. The incident caught the attention of the national media for a week or two and then faded into obscurity.

Countermeasures: Big 5 Forensics

Don't always think of technical consultants as individual, freelancing geeks with a penchant for computer security. Computer forensics is starting to become a hot commodity these days, and large corporations are cashing in on the demand.

For example, accounting giant Deloitte & Touche maintains a Boston-area facility dubbed the "War Room." The laboratory has more than half a million dollars of sophisticated computer hardware used for client computer investigations. Technicians can recover damaged hard drives and sift through bytes looking for incriminating evidence. The technicians have dealt with everything from white-collar crime to investigations relating to homicide.

Handling around 250 cases a year, business is booming.

Although as a general rule, private eyes don't tend to have the technical skills that other types of spies may have, one skill many excel at is social engineering. Called "pretext" in the PI and law enforcement business, social engineering is conning and sweet-talking information out of someone. Taking advantage of human nature can be just as damaging as the most sophisticated technical attack.

CONSULTANTS

Businesses and law enforcement are increasingly realizing that when it comes to network intrusions and electronic evidence gathering, they may not internally have the necessary experience or skills to be effective. The computer security consulting industry has grown tremendously over the past several years in response to an increasing number of computer attacks as well as media hype.

Highly skilled technical consultants are being used to find spies and plug holes to prevent them from stealing information, and the consultants are also being used to conduct forensic examinations of computers. Typically, consultants have computer science or similar degrees and various industry certifications.

Of course the skills required to catch a spy can also be used for espionage itself. Although most private investigators and consultants are ethical and abide by the laws that protect you from electronic spying, there are always a few exceptions who operate outside the law to earn their paychecks. Unethical consultants have the potential to be some of the most difficult spies to detect because of their skills and insider knowledge.

Spooks — Government-Sponsored Intelligence Gathering

When you say the word "spy," most people think of bona fide, card-carrying, cloak-and-dagger government agents. In the spy business, they're known as spooks, and the spooks that practice what has been called the world's second oldest profession, at the behest of a government, are typically pretty good at what they do.

In most cases, spying is pretty boring, tedious work. Forget James Bond or even Austin Powers for that matter. Spying is about collecting both open source and classified information, trying to put the many pieces of a puzzle together to make a guess at what's happening and then perhaps how to affect change for a government's benefit.

Traditionally, countries' intelligence agencies have been pitted against each other trying to ferret out political and military secrets, and although that is still the case, intelligence agencies all over the world have been scrambling to find new ways to justify their existence with the end of the Cold War. Across the board, the two new missions are economic intelligence and, more recently, the fight against terrorism (which has received a great deal more emphasis).

Intelligence-gathering operations are either specifically targeted or more generalized in approach (for example, seeking specific information about a certain type of missile versus gathering general data on an entire missile defense system). If an intelligence agency is interested in information you have, time will be spent researching your vulnerabilities and how best to covertly obtain the information.

Programs such as ECHELON take more of a vacuum cleaner approach. E-mail and electronic communications that travel over the Internet are collected in bulk, stored, and then analyzed for key words of interest. Also, since ECHELON is a cooperative data-sharing program, the need for probable cause and warrants is circumvented when, say, Australia collects data that relates to a United States citizen and then passes it on to a U.S. intelligence agency.

x-ref

For a complete discussion of ECHELON and other U.S. government computer surveillance programs, turn to Chapter 13.

If a government intelligence agency ever does take an interest in you or your company, prepare for the possibility of having a large number of resources (skilled technicians, hardware, and spies) used against you.

DOMESTIC

The Intelligence Community is a group of 13 government agencies and organizations that carry out the intelligence activities of the United States government. Agencies that spy or counterspy include the Department of State, Department of Energy, Department of the Treasury, Federal Bureau of Investigation, National Reconnaissance Office, National Imagery and Mapping Agency, Marine Corps Intelligence, Air Force Intelligence, Navy Intelligence, Army Intelligence, National Security Agency, Defense Intelligence Agency, and Central Intelligence Agency.

Up until the mid-1970s, the CIA and other members of the Intelligence Community illegally spied on Americans. Despite being statutorily prohibited from doing so, the CIA kept tabs on thousands of citizens with Operation CHAOS, a program originally designed to gather intelligence on Vietnam War protestors, student activists, and black nationalists. The Church Commission (a Senate investigative panel chaired by Senator Frank Church of Idaho) revealed many of these abuses, and domestic surveillance of Americans was greatly curtailed. However, with the September 11, 2001 terrorist attacks and passage of the USA Patriot Act, discussed in detail in Chapter 2, the Intelligence Community now has more powers to conduct espionage activities against citizens. Whether the loss of personal rights provides more security or the Intelligence Community's increased power allows it to unjustly abuse private citizens, as in the past, remains to be seen.

x-ref

The Church Commission hearings were extremely broad in scope; assassination attempts of foreign leaders, overthrowing governments, illegal FBI and CIA domestic surveillance. For more information see *Inside the CIA — Revealing the Secrets of the World's Most Powerful Spy Agency*, by Ronald Kessler.

Although the CIA and NSA have stated that they don't perform economic espionage, anyone even slightly clued into the intelligence business knows that they do. In 1995, shortly after the CIA Director said the agency didn't engage in business espionage to benefit American corporations, five CIA agents were expelled from France for doing just that. There are allegations that the NSA intercepted faxes and telephone calls from foreign businesses to give Boeing and Raytheon a competitive advantage during high-stakes bidding.

American intelligence agencies excel when it comes to surveillance technology. They are very good at intercepting and collecting information, particularly when it's digital. This is one of the reasons the Al Qaeda terrorist network is using old-fashioned, nonelectronic communications methods in addition to high-tech e-mail and satellite phones.

FOREIGN

It's in the best interest of a nation if its businesses have an advantage over foreign competitors. Countries such as China, South Korea, France, and Israel have known this for a long time and have successfully used their intelligence services to covertly gather economic information that can be passed on to large corporations within their borders. They're not as prudish as the U.S. in trying to deny it, either.

Spies: Project RAHAB

Since the mid-1990s, rumors have swirled around the computer underground and security communities about German government-sanctioned crackers involved in an operation codenamed RAHAB.

RAHAB refers to the name of a Biblical prostitute and spy (commonly known as Rahab the Harlot). According to various sources, around 1987 a group within the German Federal Intelligence Service (the Bundesnachrictendienst, or BND) started a covert operation designed to penetrate networks and databases and steal technical and economic information. Supposedly the project broke into computers in Russia, the United States, Japan, France, Italy, and the United Kingdom. Some of its accomplishments included compromising DuPont's corporate networks as well as cracking the banking industry's SWIFT secure transaction protocol (which meant the cracker could eavesdrop on financial transactions or create bogus transactions to shift money from one account to another).

Very little substantiated public source information exists about Project RAHAB, but if the few tidbits are true, it presents an interesting glimpse at foreign state-sponsored espionage during a period when large corporations increasingly started to use computers.

The American Society of Industrial Security conducts occasional surveys of economic and industrial espionage incidents experienced by U.S. businesses. In a 1998 survey, foreign countries perceived as key threats (in order of highest threat) included China, Japan, France, the United Kingdom, Canada, Mexico, Russia, Germany, South Korea, and Israel.

During the Cold War, there were clear distinctions between friends and enemies. Today, the situation isn't as apparent. The majority of countries engaged in economic espionage against the United States are our political allies. For example, there are reports of the French intelligence service bugging first- and business-class seats on Air France jets to eavesdrop on private conversations and snooping through laptops left in hotel rooms by American business visitors.

If your business activities take you abroad or if you come in contact with foreign nationals who take an interest in your company and products, give some thought to the potential of economic espionage.

Criminals — Ill-Gotten Gains

Although any spy that breaks a law is a criminal, "criminal spies" tend to be opportunistic data thieves. They conduct computer espionage, seeking information that helps them make an illegal profit or create some personal gain. Criminals fall into two categories: crackers and members of organized crime.

CRACKERS

Crackers are people who illegally break into computers. (I use the word "cracker" instead of the more widely used "hacker," which is an old-school complimentary term for someone who is technically clever and skilled, but doesn't necessarily break any laws.) Crackers are usually interested in financial information, particularly credit card numbers, and accounts and passwords that will allow them to break into other systems. They also may be malicious and erase files or publicize confidential information. Crackers range from "script-kiddies" (people with minimal technical skills who use automated tools and scripts to remotely break into computers) to more experienced, to unscrupulous Internet service provider administrators, to skilled professionals who understand the intricacies of operating systems and network protocols. There tend to be more script-kiddies than pros out there, and it's fairly easy to thwart the kiddies' attempts at spying.

ORGANIZED CRIME

Although you never see anyone on *The Sopranos* involved with computer espionage, organized crime has seen the future and it is digital. Computers offer all sorts of ways to illegally make money, and eavesdropping is one of them. Organized crime is mostly interested in financial and personal identity data that can be used for fraud and information that can be used in helping to plan other crimes — computer-related or not. Organized crime is in many ways like law enforcement in terms of adopting technology. Most old-school criminals won't be that technically skilled, but as new generations replace the old, the potential for more computer espionage perpetrated by organized crime increases. The one exception to the old-fashioned goodfellas is the drug cartels, which have been using skilled technicians and state-of-the-art technology for years, both to protect their own infrastructure and spy on their opposition.

Spies: Computer Spying, Colombian Style

The Colombian drug cartels have spent billions of dollars on building sophisticated computer infrastructures. In 1994, Colombian police raided a condominium complex in Cali. They found a $1.5 million IBM AS400 mainframe computer with half a dozen monitors connected to it. Dubbed the "Santacruz computer" after Cali Cartel frontman Jose Santacruz Londono, the machine was shipped to the United States for analysis. Reports on what technicians found on the computer are classified, but information has leaked out through the years.

The computer had a database of residential and office phone numbers of U.S. diplomats and agents (both known and suspected U.S. law enforcement, intelligence, and military operatives) based in Colombia. In addition, the phone company was supplying the Cartel with complete records of all telephone calls in the form of the originating and destination phone numbers. The Cartel's intelligence arm then used custom-designed software to cross-reference the phone company records against their own list of suspected law enforcement, military, and intelligence officials or agents to find out the phone numbers that these officials were calling or the phone numbers that were used to place calls to the officials. These phone numbers were then correlated back to addresses and names, giving the Cartel a list of people who were possibly informing on them.

Law enforcement officials haven't said what happened to the informers that the Santacruz computer found, but considering the Cartel's penchant for violence, it seems reasonable to believe suspected informants were tortured to reveal information or killed outright. There are no public sources that estimate the potential loss of life that resulted from the Cartel's computer operation.

Whistleblowers — For the Public Good

Another type of spy, generally considered benevolent (depending on whom he is spying on) is the whistleblower who exposes corruption and unsafe practices for the public good. Of course, whistleblowers wouldn't exist without the media, who give them a chance to tell their story, and sometimes engage in independent, investigative whistleblowing of their own.

Whistleblowers are typically insiders who have access to evidence of some wrongdoing. They might also be journalists working on a story. Whistleblowers often have above-average technical (Internet and computer-related) skills, which they use to their advantage in exposing wrongs. With the advent of the Internet, whistleblowers have an easy way to pass their knowledge along and yet remain anonymous. Through temporary e-mail accounts and anonymous remailers, a spy can reveal information to a third-party source without much fear of discovery. Embarrassing and damning company e-mail and instant-messaging logs are being exposed on the Internet with a greater frequency.

If you work for a company such as Enron, you may have potential whistleblower spies in your midst — which might not be a bad thing.

Spies: Cryptome.org

John Young is a New York architect who strongly believes in personal privacy and exposes the secrets of those who invade the privacy of others. He runs the cryptome.org Web site, a clearinghouse of esoteric information related to intelligence agencies, government, privacy, cryptography, surveillance, and freedom.

Since 1996, Young has collected a remarkable amount of whistleblowing information from anonymous sources. This information includes lists that blew the cover of foreign intelligence agents; a customer list from a surveillance hardware company with names of government, military, and law enforcement employees; copies of disreputable monitoring software; and various open and closed source government documents.

Cryptome.org has gained an international reputation for publicizing tantalizing details for those who study espionage. In addition to privacy advocates, spy buffs, and investigative reporters, various intelligence agency *bots* (automated software robots that collect data) frequently visit the site, downloading new information for government analysts to study in an attempt to find leaks or discover pieces in some larger intelligence puzzle.

Friends and Family — with Friends like These . . .

Although spying is usually thought of in a business or government context, the reality is that the home computer is probably the most vulnerable when it comes to espionage. However, the threat is not from crackers who break in through broadband connections, but rather from family and friends.

Maybe they suspect you of doing something wrong and are looking for evidence. Maybe they are just curious about what's on your computer and are nosing around for information. As computers have become integrated into our lives, they can cast a light onto parts of our personal lives we want to keep private.

For the most part, friends and family generally have the lowest amount of technical skills compared to other spies, and they typically rely on browsing through file directories and using easy-to-install-and-run commercial and free software.

x-ref

Keyloggers are probably the biggest threat when it comes to family spying. These surveillance tools are discussed in detail in Chapter 8.

ROOMMATES

The number of roommates and boarders in the United States is on the rise. In the past, it just used to be college roommates, but now because of tight economic times, 20- and 30-something-year-old couples that have purchased their first home are increasingly taking in boarders to help offset

Busted: Best Friends?

Nicholas J. Suchyta, 19, shared an apartment in Bay City, Michigan with a 19-year-old woman. The female roommate said she and Nicholas had been best friends since grade school.

In January 2002, acquaintances of the woman told her they had seen live video of her on the Internet having sex with her 18-year-old boyfriend in Suchyta's apartment. The woman searched through Suchyta's computers and found nude pictures of her. She then complained to the police who found a hidden Web camera attached to her computer and four files of the teens having sex.

In May 2002, Suchyta was arraigned on two counts of installing eavesdropping devices and two counts of divulging information from eavesdropping devices. He had previously been in trouble for alleged cracking activities while employed by a local school district. In that case, Suchyta and his parents sued the school for defamation of character, invasion of privacy, intentional infliction of emotional distress, and gross negligence, as a result of Suchyta being branded a "hacker."

The case is scheduled to go to trial in late April 2003. If Suchyta is convicted, he faces up to two years in prison as well as a fine.

costs. Whether you have a school dorm roommate or are sharing a house or apartment with someone, an unsecured computer is a tempting target for snooping.

SIGNIFICANT OTHERS

Trust seems to be passe these days. Jealous boyfriends, girlfriends, husbands, and wives are heading to their current and former significant others' computers in an attempt to find evidence of real or virtual unfaithfulness.

Maybe it has something to do with the relatively anonymous and easy way that electronic relationships can be found and maintained through e-mail, instant messaging, and chat rooms, or perhaps the media is encouraging interest and experimentation with lurid coverage of online affairs and cyber-sex. Or possibly all of those advertisements on Web sites for spy software designed to catch your spouse electronically cheating gives people doubts about their relationships. Whatever the reason, "significant other" computer spying is turning into a booming business.

PARENTS

When the Internet first started to become popular, parents were concerned about keeping their children away from adult-oriented Web sites. Now in addition to Web sites, kids have access to chat rooms, instant messaging, and personal e-mail accounts. Media hype about the dangers of the Internet has caused some parents to take an active interest in spying on their children's computer activities. Web-filtering software now includes features that monitor chatting and e-mail, and keyloggers are advertised to help parents discover what their children are up to while online.

Busted: 'Til Keyboards Do Us Part

In 2001, Steven Paul Brown separated from his wife Patricia, but the separation wasn't amicable. Brown installed a commercial keylogger program called eBlaster on his former wife's computer. The program recorded her e-mail, Web surfing, and online chatting and then e-mailed a copy of her activities to Brown. Brown made the mistake of mentioning the contents of an e-mail exchange between his former wife and a friend. His wife became suspicious, and the Michigan Attorney General's High Tech Crime Unit investigated.

Brown was charged with installing an eavesdropping device, eavesdropping, using a computer to commit a crime, and having unauthorized computer access (all felony offenses). He faces penalties of up to five years in prison and fines of up to $19,000.

CHILDREN

A significant portion of the adult population isn't very savvy when it comes to computers. Although they can perform common tasks such as using a word processor, sending e-mail, and surfing the Web, they've never had to develop more esoteric skills, especially those that are security-related. On the other hand, their children have grown up on the Internet, many collecting a remarkable set of technical skills that go way beyond those of their parents'.

Kids actually pose a significant threat as junior spies — spy tools are discussed in e-mail and chat rooms and then readily downloaded from cracker Web sites. A savvy 12-year-old can easily install a keylogger on the family computer and eavesdrop on whatever Mom, Dad, brother, and sister are up to. Privacy involving financial transactions, connections to work computers, e-mail, and Web surfing can easily be compromised.

Determining Your Level of Paranoia

Sun Tzu said that to prevail in battle, you need to know yourself. So the question is, with all of these potential spies at work, at home, and seemingly everywhere you look, just how paranoid should you be?

Part of the answer is to know yourself (or in the case of a business, your organization). Here's a quick test that might help. There's no time limit, so give the questions some thought.

- ✓ Can you tell the difference between a credible probable threat to your computer or network versus an unfounded possible one? If you're big into black helicopters, U.N. takeovers, and unfounded government conspiracies, answer no.
- ✓ Can you put on a spy's cloak and use his dagger to try to poke holes in your computer system? Thinking like a bad guy is important for understanding your weaknesses. You'll be asked to do this throughout this book.

- ✓ Are you willing to put policies in place to ensure your computer's security? Security policies are extremely important, but they go beyond the scope of this book, which focuses on espionage tactics and countermeasures.
- ✓ Will you follow the policies you created? If you think security policies are a waste of time or too much of a burden to follow, answer no.
- ✓ Are you the type of person that's willing to put up with a little inconvenience for increased security? The general rule of thumb is that as any type of security increases, convenience and usability typically decrease.

If you answered yes to all of the questions, you're not paranoid, but simply prepared and can reduce your chances of being spied on.

If you answered yes to most of the questions, examine the questions you answered no to. There might be a few issues holding you back from being entirely effective in preventing computer espionage.

If you didn't answer yes very often and someone is planning on spying on you, he could be very successful. If you're concerned about this, it might be time to bring in some outside help.

Protecting yourself from computer spying is somewhere between blissful ignorance and wearing a tinfoil hat to keep the radio waves out of your brain. You need to find the right balance.

Risk: Color Codes

Colonel Jeff Cooper, a prominent firearms instructor, developed a widely used color code for awareness and preparedness based on his experience in the Marines. (Recently, the U.S. Government has implemented a similar color code for homeland defense purposes.) Cooper breaks his system into the following four colors:

- ✓ **Condition White.** This is a complete lack of awareness of any possible threats or information that might lead you to believe there is a threat. Most people go through their lives in this condition.
- ✓ **Condition Yellow.** This is relaxed awareness, much like you have when you're driving defensively. You're aware of your environment and things that seem out of place. Code yellow awareness shouldn't be that taxing, and with training you should be able to be in this state during your waking hours.
- ✓ **Condition Orange.** This is an awareness of a potential threat that makes your antenna go up and starts you planning on options for dealing with the threat.
- ✓ **Condition Red.** This is when you identify a real, specific threat and then take control of the situation.

Although the color code is primarily designed for self-defense, it is equally applicable to a mindset for preventing computer spying. Are you willing to move to a Condition Yellow state with your computer and then be ready to escalate to higher levels if need be?

Risk Analysis 101

At the start of this chapter, Sun Tzu said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." That's what risk analysis is all about. It quite simply involves identifying the most probable threats, analyzing the vulnerabilities, and determining what countermeasures should be put in place.

Before continuing, it's important to have a good understanding of these three key terms:

- ✓ **Threat.** A threat is something that poses danger. Throughout this book, spies are the key threats as they present a danger of compromising information on computers.
- ✓ **Vulnerability.** A vulnerability is a condition that causes something to be susceptible to attack. Spies look for weaknesses in security, or vulnerabilities, to exploit. For example, a spy may exploit a known buffer-overflow vulnerability in a Web server to gain access to files on a corporate network.
- ✓ **Countermeasure.** A countermeasure is an action taken to offset another. Quite simply, countermeasures prevent exploits. An example of a countermeasure is installing a vendor's patch to prevent a Web server buffer-overflow attack.

Let's go through an imaginary risk-analysis example.

Your Aunt Sara had a prize-winning chocolate cake recipe that was the envy of everyone in the county. With her final breath, she gave you the recipe and told you to never reveal the ingredients to anyone. You've kept the recipe on your hard drive ever since, and despite bribes and threats you've never shared it with anyone.

Is it possible that government spies are interested in your Aunt Sara's recipe? Because anything is possible, does that mean you should withdraw your life savings, hire armed guards, install a retina scanner on your PC, and shield your office to prevent stray electromagnetic emanations from being intercepted by men in black vans with TEMPEST intercept equipment?

Although it's possible that there's a rogue CIA agent with a sweet tooth that heard about Aunt Sara's cake, it's not very probable. So scratch off a government-sponsored intelligence operation as a threat, and because now that you don't have to worry about all the sophisticated tools and methods associated with state-sponsored espionage, you can fire the armed guards and return the retina scanner and TEMPEST shielding. (Of course, everything might change if Aunt Sara's real name was Natasha, and she had this funny little tattoo on her arm with a sword and shield and tiny little letters underneath that spelled out KGB.)

A more realistic threat comes from your sister-in-law Christina, who's been after the recipe for years. Christina and her family show up every year for Thanksgiving and Christmas, and when her kids get bored, you send them off to your office to play computer games. Little Billy is especially good with computers, and over dinner you get into long discussions with him about various Microsoft security holes. You've never really trusted Christina after the nasty incident involving Aunt Sara's silverware. So now what's the threat, what are the vulnerabilities, and how should you respond?

If you thought Billy's mom might put him up to snooping through your computer to see if he can find the prize-winning cake recipe, you've identified a probable threat. You know Billy is a whiz when it comes to Microsoft operating systems, so you've cleverly put the games on the Windows XP machine while the recipe is safely encrypted with Blowfish on a Linux laptop, which is locked in your bedroom desk drawer. You've identified the vulnerability and came up with several countermeasures. (This book is full of espionage vulnerabilities and countermeasures.)

There are all sorts of methodologies for performing risk analysis. Some use mathematical models, assigning numeric values to different types of and duration of risk. Statistical probabilities can be derived that rank the potential of different types of risk so you can make better decisions about protecting yourself from different threats.

Five-Step Risk Analysis

Lots of time can be spent discussing risk analysis, but because this book is primarily about computer spying, here's a quick, five-step model to help you perform a simple yet effective computer espionage risk analysis.

Let's discuss each of the steps and then apply them to two fictional organizations with different situations:

- ✓ e4bics Corporation, a high-tech startup developing a Voice over Internet Protocol (VoIP)
- ✓ No More Violence, a nonprofit support organization for battered women

DETERMINE WHAT YOU HAVE

To start out, what's on your computer that has value? This information is either stored on a computer's hard drive (or some other storage medium) or is transferred between computers if you're using the Internet or a local area network (LAN). Although some economists would argue that you could assign a monetary value to everything, value doesn't necessarily equal cash in this case. Although the information could have a tangible value (such as a credit card number or trade secret), it also might not. Perhaps it is some bit of evidence that if discovered could send you to prison or destroy your relationship with someone.

- ✓ e4bics Corporation has just completed work on a new communications server designed for voice-centric and multimedia technology. The proprietary software and hardware dramatically beat all of the competition in terms of performance and pricing. The official marketing rollout is planned for six months from now, but industry rumors have been circulating about the product. Any information that has to do with product R&D, marketing, and sales is valuable for obvious reasons.
- ✓ In an attempt to streamline its operations, No More Violence has started to use a computer database to track women that the organization is supporting. Part of the organization's mission is to find temporary safe places for domestic-violence victims to live. The database contains women's names, addresses, and other personal information. All of this data is extremely sensitive and thus valuable in a nonmonetary way.

LIST WHO MIGHT WANT IT

Now, consider who might want whatever it is you think has value. The first part of this chapter contains a rather long laundry list of people who typically spy, so you should have some ideas about the usual suspects. Remember to categorize your adversaries as probable rather than possible, so you can focus your energy on exploits that are *likely* to happen and not ones that merely *could* happen. Keep your imagination in check and your paranoia well founded.

- ✓ In e4bics' case, any number of large or small competitors would love to have the inside scoop on their newly developed technology. This includes companies both inside and outside the United States. The company's executives have recently been approached by representatives from several large competitors asking to partner on future projects, but the nondisclosure agreements seem pretty one-sided in favor of the competitors.
- ✓ Some of the women that No More Violence supports have violent former partners who currently have restraining orders filed against them. With a pattern of continued abuse and harassment, a number of these men want to find their former wives and girlfriends.

DECIDE HOW BAD THEY WANT IT AND HOW MIGHT THEY GET IT

Let's say the adversaries you've identified know or suspect that valuable information resides on your computer. How bad might they want it, and how might they try to get it? When answering this question, consider the security measures you already have in place, and how effective they will be in stopping or slowing down an adversary. Also, remember to keep suspected attacks probable, not possible. Although it's worthwhile to spend some time brainstorming all sorts of creative attack possibilities, time is a finite commodity, and it's a better investment to first focus on the probable.

- ✓ Because e4bics' new product could have a significant impact on the industry, the company is quite concerned about economic espionage. J.D., the company's chief engineer, formerly specialized in penetration-testing work for the Air Force and has a long list of ways a competitor could try to get e4bics' trade secrets, including dumpster diving, social engineering, breaking into the offices after hours, or trying to enter through some hole in the networks.
- ✓ One of the women that No More Violence helped is named Sue and is a network administrator with a background in security. In talking with the organization's office manager, Sue mentioned that someone could break in and steal the database files or the entire computer. Because the Windows XP desktop is connected to the Internet through a cable modem, a spy could try to remotely break in and access the database. The office manager knows that one of the women's former husbands has a burglary conviction and another's former boyfriend used to crack e-commerce Web sites for fun. The database is running on Microsoft Access, and is protected using the program's built-in encryption. Sue points out Access's weak encryption and tells about her personal experience of discovering the lost password for a protected database in a matter of seconds using a free cracking program.

SPECULATE ABOUT WHAT HAPPENS IF THEY GET IT

Imagine the worst-case scenario. Your adversary manages to get the information on your computer. What are the probable implications and consequences? Try to be as detail-oriented with this question as possible, looking at the present and into the future.

- ✓ In e4bic's case, the impact of having proprietary information compromised depends on just what it is. If sales data were stolen, competitors could target accounts that the company is in the process of developing. If marketing plans are revealed, a competitor could develop a counterstrategy. If a competitor gained access to e4bics' R&D crown jewels, the company's planned competitive edge could be weakened if not entirely crippled. As a small startup, the company and all of the employee's livelihoods could be at stake.
- ✓ The worst-case scenario for No More Violence is relatively simple. If the database with the women's names and addresses fell into the wrong hands, it could put the safety and perhaps the lives of the organization's clients in jeopardy at any point after the information was compromised.

DETERMINE HOW YOU SHOULD PROTECT IT AND WHAT THE COST IS

You've now identified what you have that is valuable, who might want it, how bad they might want it, how they may try to get it, and what happens if they succeed. The final step is to factor all of this together to create a plan that will protect that item of value.

Because you probably don't have an infinite budget to spend, you need to make some conscious decisions about the levels of security you'll use to protect the information. Don't think only in terms of how much a security product costs. Remember that there is a negative correlation between security and usability. As security levels increase, it becomes more difficult for users to perform their everyday job duties, which can incur another cost to the company — namely, a slowdown in efficient, quantitative output.

- ✓ J.D. knows that there's a lot riding on keeping his e4bics's information safe. He first performed a risk analysis and identified vulnerabilities a spy could exploit. He then came up with a planned series of countermeasures to plug the vulnerabilities. Finally, he developed a strict security policy that addressed both computer and physical security issues. The CEO and investors understood the importance of information security and approved J.D.'s security budget and plan. (In real life, you'll have much more of a challenge convincing the suits that the threat of espionage is real and measures should be taken to prevent it, but because this is a hypothetical case, let's have a happy ending.)
- ✓ After discussions with a friendly police officer and Sue, the No More Violence office manager planned to beef up physical security by installing both new locks and a monitored security system. A NAT router (NAT stands for Network Address Translation; it provides transparent access to the rest of the IP network, usually the Internet, through one gateway computer) was purchased to protect the computer from Internet intruders, and current security patches were applied to the Windows operating system. Finally, the popular and secure Pretty Good Privacy, also known as PGP, strong encryption utility was used to protect the database. No More Violence doesn't have a very large budget and its staff doesn't have many technical skills, so all of the security measures were affordable, as well as fairly unobtrusive so as not to discourage their use.

Summary

You now should have a better idea of who your enemy (a spy) is, whether you have the right stuff to take him or her on, and how to go about assessing the risk of computer espionage.

Throughout the rest of this book, you will be exposed to a number of tactics that spies use to compromise data. When you read about these spy tactics, pretend you're a spy, and see how effective some of these attacks would be on you, your business, or your organization. Always consider whether an attack is probable or possible, though. All the espionage tactics described are possible, but your own personal situation will make them either more or less likely.

As new vulnerabilities are discovered on a daily basis, with some taking a long time to percolate into public view, it's impossible to create a perfectly secure computer. There's an old saying in the security industry that the only way to absolutely secure a computer is to cut all the cables, fill it with cement, and then bury it. Then it still might not even be secure.

Your job should be to minimize the risk of computer espionage as much as possible. You can't be 100 percent certain that you can keep a spy from accessing information or evidence, but you can make his job as difficult as possible. Hopefully, the cost in time and effort will cause him to look elsewhere for other targets.