

Who's Stealing Your Information?

In today's enterprise, the answer is everyone. Here's what (and who) to watch out for, and how you can better protect your company's jewels. **BY DOROTHY E. DENNING**

Companies in the United States could be losing more than \$250 billion annually to information thieves, according to a 1997 American Society for Industrial Security (ASIS) survey of Fortune 1000 firms and the 300 fastest growing U.S. companies. More than half (56 percent) of the 172 companies responding to the survey reported at least one attempted or suspected information misappropriation. Over a 17-month period, some 1,100 documented incidents of intellectual property theft were identified, worth an estimated \$44 billion. And the problem may be getting worse: The estimated dollar losses were five times greater than that reported in the previous ASIS survey.

If these statistics make you feel a little insecure, they should. No matter what industry or economic sector your organization is in, it produces, maintains and transmits information, intellectual property and trade secrets that others would love to get their hands on. The problem is, the threat is multidimensional, difficult to pinpoint and therefore difficult to prevent.

Today, your organization is vulnerable to attacks by people both inside and outside the corporate walls, breaches both physical and electronic, sophisticated scams as well as unintentional leaks, and both legal and illegal competitive intelligence-gathering efforts. Worse yet, even when you can prove intellectual property theft, the law may not always work to your company's advantage.

So what do you do? First, you need to recognize the scope of the problem—who's stealing your information, and how they're going about it.

Employee Turned Traitor

The ASIS survey confirmed what information security experts have been saying for years: The single greatest threat to corporate intellectual property is trusted insiders—current and former employees, temps, onsite contractors, consultants, partners and suppliers.

Trusted employees. Trade secrets are routinely smuggled out of companies and sold to a waiting customer or information broker. Just last month, a U.S. nuclear scientist working at the Los Alamos National Laboratory was accused of disclosing top-secret nuclear weapons technology to China in the late 1980s. As *Information Security* went to press, the extent of the espionage was still unknown, though one U.S. official said the Chinese

were able to "telescope the time" required to develop such advanced technology and "could not have done it without information from the U.S."

In another case involving China, in 1994 a highly trusted employee of Ellery Systems in Boulder, Colo., allegedly used the Internet to transfer \$1 million worth of software to a competing Chinese firm.

The accused perpetrator, a Chinese national, had been granted asylum in the United States following the Tiananmen Square incident. Shortly before transmitting the code, he had traveled to Beijing, allegedly to visit his sick mother. But while he was there, he signed a letter agreeing to provide the source code in exchange for \$550,000. When he returned to the U.S., he tendered his letter of resignation. The next day, he transferred the software.

Duped employees. Some employees have been bribed or seduced into giving away secrets. In his book *Corporate Espionage*, Ira Winkler tells about a German spy named Karl Heinrich Stohlze who seduced a lonely woman who worked for a Boston biotechnology firm, eventually convincing her to leak corporate secrets. Stohlze, who had been sent by Germany's intelligence agency, the Bundes Nachrichten Dienst, skillfully exploited the relationship, telling the woman he would be transferred back to Germany if she did not get copies of certain documents for him. Not wanting to lose him, the woman supplied him with the information he sought, including DNA research methods and information about the status of company projects.

To keep the information flowing, Stohlze used blackmail in addition to romance, according to Winkler. "I may have made a mistake," he told her. "I told one of my associates in Washington what you are doing for me.... The trouble is that Hans is crazy. He does not want to be reassigned; his family is settled here. I fear if the information stops coming, he just might contact your company and show them the documents, just to get even with you." Shortly after that, the woman was caught and fired, although no charges were brought against her. Stohlze was not prosecuted and was later seen working other assignments in Western Europe.

Former employees. While current employees constitute the greatest threat to corporate trade secrets, former employees are not far behind. In 1993 General Motors accused its former head of worldwide purchasing, Jose Ignacio Lopez, and seven other former employees of stealing 10,000 proprietary GM documents and computer disks when they defected to Volkswagen. The stolen materials included details of a secret new car model, future sales strategies and purchasing lists. In 1996, GM sued Lopez and VW, causing VW's stock to drop. Ten months later, GM was awarded \$100 million in damages.

Foreign Affairs

While insiders pose the greatest threat to the company's jewels, outsiders are a close second. But even then, insiders may be unwitting accomplices.

Info requests. Based on reports sent to the U.S. Defense Investigative Service (DIS), unsolicited requests for information are the most frequently used modus operandi for foreign collection of U.S. technology information. In 1996, such requests surpassed all other collection methods by a nearly three-to-one margin.

Phony foreign requests for information or "partnering" arrangements can take many forms: letter, fax, phone call or e-mail. Foreign operatives may request free samples of software and working models. Or, they may offer, unsolicited, to work as sales agents, consultants or representatives in foreign countries. The foreign operatives frequently word their messages to appeal to cultural commonalities (*see box, p. 23*).

Visits. Foreign operatives may even try to schedule meetings at U.S.-based companies under the guise of "mutual information-sharing." Then, they'll arrive with last-minute or unannounced persons, try to wander away from approved locations or initiate conversations beyond the scope of the visit. They may pressure the host into becoming conciliatory or use social engineering techniques to get information from employees. While these seem like obvious ruses, the threat is real: In a surprising number of cases,

insiders give away information they would not have had they realized the motives of their assailants.

Joint ventures and licensing. In order to break into a foreign market, a U.S. company may enter into a joint venture with a foreign firm. Doing so, however, often requires the transfer of proprietary secrets—if not as a condition of the contract, then as a matter of practical necessity. The problem is, once the foreign firm acquires proprietary technology, it can use it to make a competitive product. India, for example, is said to use compulsory licensing for pharmaceuticals. Companies wanting to sell pharmaceuticals in India must license use of the technology to an Indian company. The Indian company may then turn around and begin marketing a similar product.

Surveillance Technologies

Although most intellectual property is stolen through low-tech means, surveillance technologies also pose a threat. For example, in 1988 France's Direction Générale de la Sécurité Extérieure (DGSE) allegedly sent a four-man team to Seattle to intercept test data and personnel communications during flight tests on Boeing's new 747-400 airplane. Information collected on the 747's new computerized navigation system was allegedly used in a similar system in the Airbus A340.

While this incident happened more than a decade ago, an independent report released last year by the Commission for the Control of Security Interceptions suggests that illicit state-sponsored surveillance continues today in France. The report says that more than 100,000 telephone lines are tapped illegally each year in the country, with state agencies behind most of the eavesdropping. France, of course, is not the only country to employ surveillance technologies, and even the U.S. has been accused of such spying.

Electronic Break-ins

Computer penetrations are a serious threat to intellectual property. A recent high-profile case involving competing investment brokers Reuters Holdings PLC and Bloomberg LP demonstrates the reality of this growing threat.

More than \$6.5 billion is spent annually on computer terminals that Wall Street traders use to get up-to-the-second bond and equity prices and currency values. These computers contain sophisticated, proprietary software applications and tools that allow traders to analyze investments and predict current trends. Even though Reuters had more than a century's head start on the trading room floor, Bloomberg's new trading tools were considered superior. So Reuters founded a subsidiary called Reuters Analytics to develop a competitive product.

Rather than devote millions to product R&D and testing, however, Reuters Analytics took a different tack. In January 1998, reports alleged that the subsidiary had commissioned a consulting company to break into Bloomberg's computers. As a result of the breach, the consulting company reportedly obtained information about Bloomberg's operating code, the underlying software that governs the functioning of Bloomberg's data terminals. This information was then passed on to Reuters Analytics, as well as to the parent company's London headquarters.

Often, though not always, a computer attacker holds (or has held) a position of trust within the targeted organization. While the method of break-in was not disclosed in the Reuters-Bloomberg case, sources said former Bloomberg employees working for Reuters Analytics or the consulting company may have been involved.

Competitive Intelligence

The Reuters/Bloomberg case illustrates just how far companies will go to gain

access to the secrets of their competitors. However, not all efforts to obtain competitive information are illegal. In fact, many organizations have competitive intelligence units that gather information through legal means. An April 1998 article in *Forbes* tells how IBM CEO Louis Gerstner, shortly after taking over the top spot at Big Blue, set up a squad of a dozen intelligence teams. The teams are part of an extensive "human intelligence network" that targets competitors' consultants, suppliers, customers and even employees. Information gathered by the teams is placed in a central database, which is accessible to 450 of the firm's top executives, *Forbes* said.

An October 1996 *Business Week* article reported that brokerage firm Charles Schwab & Co. set up an intelligence program in 1994 to keep tabs on competitors by paying consultants to visit rivals' facilities, hiring competing firms' workers and quizzing customers. In the same article, Robert Flynn, former chairman and CEO of Nutrasweet, estimated that the work of his company's competitive intelligence unit was equivalent to at least \$50 million a year.

Some firms send their employees to conferences where they learn the tricks of the trade. *Forbes* tells the story of John Nolan, a former military intelligence officer who now trains corporate spies for the Centre for Operational Business Intelligence. Nolan's students learn that a good spy is a bit of an actor, appearing innocent and friendly and knowing when to act dumb. They are taught to exploit the weaknesses of their targets. Disgruntled factory workers, for example, can be enticed into whining about management and revealing valuable tidbits. Salespeople are especially vulnerable because their success depends on imparting persuasive information. Lawyers and executives may disclose information because they "need you to know how clever they are."

Another Nolan tip: By eliciting information in the middle of a conversation, suspicion can be avoided, because people tend to remember mainly the beginning and end of a conversation. Nolan also talks about how to ask leading questions. He tells the story of how he once discovered the profit margin of a particular defense contractor simply by asking the contractor's accountant, "So your profit margin is 40 to 50 percent?" Without a thought, the accountant corrected him, revealing the actual figure.

Although much corporate intelligence activity is considered fair and legal game, some deceptive practices—such as assuming a false identity—are regarded as unethical and sometimes illegal. In February 1996, Maxim Integrated Products, a high-tech company in Silicon Valley, sued a competitor, Linear Technology Corp., for allegedly stealing trade secrets through an employee who posed as a customer.

The Society of Competitive Intelligence Professionals (SCIP) has adopted a code of ethics that prohibits masquerading in such a manner. Under the code, members agree "To comply with all applicable laws"; "To accurately disclose all relevant information, including one's identity and organization, prior to all interviews"; and "To fully respect all requests for confidentiality of information."

Economic Espionage Act

Prior to 1996, U.S. federal law did not explicitly address trade secret theft. Prosecutors had to apply laws designed for other purposes, such as wire fraud, mail fraud and interstate transportation or receipt of stolen goods. Alternatively, they could prosecute under state trade secret laws, which emerged in the 1970s.

The laws were inadequate, however, and some thieves went free. This happened in the Ellery Systems case mentioned above. Charges against the Chinese national accused of pilfering \$1 million worth of software from the company were dropped, and Ellery itself subsequently folded.

Three years ago, Congress passed the Economic Espionage Act of 1996 to provide stronger trade secret protection at the federal level. This law made it illegal for anyone to knowingly steal or otherwise fraudulently obtain a trade secret; to copy or distribute a trade secret; to receive or buy a trade secret; or to conspire to commit any of these acts in

order to benefit a foreign government, instrumentality or agent, or to convert the trade secret to the economic benefit of anyone other than the owner.

For the purposes of the law, "trade secret" means all forms and types of financial, business, scientific, technical, economic or engineering information, provided the owner has taken reasonable measures to keep such information secret and the information derives independent economic value (actual or potential) from not being made public. Penalties can be as high as \$10 million and 15 years in prison for acts conducted to benefit a foreign government, instrumentality or agent (economic espionage), and \$5 million and 10 years in prison for acts conducted to benefit other parties (commercial espionage).

To date, several cases have been successfully prosecuted under the act. The EEA has, however, posed problems for at least one victim, the pharmaceutical firm Bristol-Myers Squibb Co. In 1997, Jessica Chou, an executive with Taiwan's Yuen Foong Paper Industry Co., and one of Chou's employees allegedly tried to steal Bristol-Myers' formula for Taxol, an anticancer drug, according to a February 1998 report in *The Wall Street Journal*. Chou asked an FBI agent posing as an information broker to find a Bristol-Myers employee willing to sell her the information. In return, the agent would get \$400,000 in cash, stock in the Taiwanese paper company and royalties from the sale of the drug. Chou also asked to see certain documents related to Taxol so she could assess the technology.

Working with the FBI, an employee of Bristol-Myers brought the documents to a meeting, where Chou and her accomplice were caught red-handed and arrested. That was when Bristol-Myers' real troubles started. Lawyers for the defendants argued that their clients had a right to see the documents. They claimed the information did not fit the definition of a "trade secret" because much of it was in the public domain, and Bristol-Myers had not taken sufficient steps to prevent its disclosure. A U.S. district court judge ruled in the defendants' favor, saying they "must have the exact processes and formulae for Taxol available to them—or at least those formulae and processes that the government will contend to the jury are trade secrets."

You can imagine that the decision did not sit well with Bristol-Myers or Richard Goldberg, the Philadelphia assistant U.S. attorney prosecuting the case. In court papers, Goldberg said, "The concept of profiting from the attempted theft would reach new heights if prosecution resulted in the transfer of trade secrets which could not be obtained illegally." Goldberg also said that if the ruling is upheld, the government will take steps, including possibly seeking dismissal of the case, to prevent disclosure of the trade secrets. If upheld, the ruling will probably affect future cases, with companies reluctant to pursue prosecution for fear of losing control over their intellectual property.

Truth in Numbers

Theft of trade secrets is one of the most serious threats facing business today. The latest CSI/FBI Computer Crime and Security Survey, released in March, found that of 12 types

of computer crime and misuse, theft of proprietary information had the greatest reported financial losses for the period 1997-1999. According to the survey, more than \$42 million worth of trade secrets was stolen from 64 organizations that were able to quantify their losses from this type of breach.

The lesson is clear: If you don't want to be the next victim, be aware of the danger, and be sure to design, implement and update a comprehensive security program that addresses the threat from all angles (*see below*).

Dorothy E. Denning, Ph.D., is a professor of computer science at Georgetown University. Dorothy is also a member of Information Security's Editorial Advisory Board. Portions of this article are taken from her latest book, Information Warfare and Security (Addison-Wesley, 1999, ISBN 0-201-43303-6).

IF IT LOOKS LIKE A SCAM...

Tip-offs that a foreign request for company information might be a scam:

1. The request offers a "multimillion-dollar" deal.
2. The sender is in a big hurry, so there is no time to check his credentials.
3. The fake sale is always "wired" so that your company won't have to compete with others for the deal.
4. The exact purpose of the request is vague, so the sender needs to know everything about your business, including capability statements and customer lists.
5. The sender demands a visit to his country at your company's expense.
6. The request is full of propaganda.

From "How to Spot a Fake," Counterintelligence News and Developments, National Counterintelligence Center, Vol. 4, December 1997.

EYE FOR AN EYE

A Modest Proposal

Many organizations have turned to computer forensics to catch the bad guys. May I suggest something a little more radical? BY WINN SCHWARTAU

Lately, it seems everyone's talking about computer forensics, the art and science of building evidence to prove past cyber-criminal acts. I'm here to suggest that the concept of forensics won't work in cyberspace. It's simply too little, too late. That is not to say we don't need forensics in infosecurity. We do. But if we rely upon forensics to protect and defend our networks, we are destined for failure.

Forensics is a logical outgrowth of physical law enforcement, which itself is doomed to fail in cyberspace. First of all, I'd like to suggest that police forces do not, in fact, "serve and protect." Rather, they react to crimes committed in the past, or if they are exceedingly lucky, in progress. The concept of police presence is one of deterrence, not protection.

Similarly, the concept of forensics is one of analyzing activities after the fact; it does nothing to protect the very networks we are pledged to defend and protect. Actually, forensics is a possible deterrent to online crime if, and only if, would-be computer criminals are made sufficiently aware of the increasing capabilities of forensic experts. By relying upon deterrence mechanisms (forensics, police presence), we fall into the same trap we succumbed to with firewalls and similar electronic defensive/protective mechanisms: our network security efforts turn out to be not terribly effective.

The concept of the Fortress Mentality, a 5,000-year-old military model, is one in which the good guys (us) try to keep the bad guys (them) out of our (physical) land or our (virtual) networks. Unfortunately, the Fortress Mentality has not worked for many reasons, not the least of which is poor administration, constantly changing network terrain, error-filled system configurations, improper applications design and an army of hacker-types who spend every waking moment searching for electronic weaknesses in our infrastructures.

Sounds sort of dismal, eh?

The Myth of Deterrence

Amidst the hoopla of apparent Internet successes, we have forgotten a fundamental principle: we don't want the crimes to occur in the first place. We really want to prevent network breaches, not study them later. We really need to keep the bad guys from wreaking havoc in our systems, not try to convince the cops that we have a case worthy of their time.

That brings up another sore point with the current approaches to network security. Deterrence doesn't deter the bad guys; it only deters the good guys. Fear of police prosecution doesn't stop the enlightened criminal when he knows full well that the odds of being caught are darned close to nil. Protection, the electronic bastion of hope that surrounds our virtual wealth, does a fantastic job of keeping the good guys at bay. But the dedicated adversary will expend his resources to find a way in—which in a vast majority of the cases, he will.

So, what are the police doing about this? Unfortunately the answer is not encouraging. Burdened by a massive lack of technical skills, insufficient budgets and manpower—not to mention the difficulty of making the transition from the physical to the virtual model—the police are able to investigate only a very small number of computer crimes. In some cases, law enforcement has placed artificial thresholds on losses that victims must sustain prior to commencing an investigation—anywhere from \$50,000 to \$1 million or more.

Paradigm Shift

For many companies, cybervigilantism has become a radical but effective approach to the forensics problem. Vigilantism, the practice of acting against an adversary without the benefit of law enforcement aid or support, brings up memories of Charles Bronson and the Death Wish series. However, according to opinion surveys conducted in January by Infowar.com, NWFusion and CNN, approximately 30 percent of respondents believe that vigilantism, in varying degrees, is an appropriate response to cyberattacks.

There are many ways to create a hostile perimeter around your networks; it's up to you (and your boss) to determine which, if any, is acceptable. If we find ourselves under attack, do we send back an angry e-mail to the aggressor? Do we merely cut off his electronic air supply through dynamic IP filtering? Do we notify his ISP and make threats of legal retaliation? Do we release hostile code (Java or otherwise) at the attackers, which in itself might be a crime? (All of these options are explored in depth at www.infowar.com.)

For all of the resources and fine minds we have in this field, we still seem to be inextricably stuck with old-style paradigms that we know are fundamentally weak. We seem willing to live with the losses and the lack of law enforcement compliance. The fact is, we have new mathematics to define infosecurity, network defense and infrastructure protection. And we have new security models and architectures to address the realities of network life. Now all we need to do is use them.

Winn Schwartau, a contributing editor to Information Security, is CEO of Security Experts and founder of Infowar.com. His latest book is Time Based Security (Interpact Press, ISBN 0-9628-8700-4-8).

5 STEPS TO FOILING INFO THIEVES

Information thieves are targeting your organization from every angle. What do you do about it?

1. Establish a security policy covering all company information.

This involves identifying proprietary information and pinpointing who is allowed to access it—and when. This policy should cover employees, temporaries, customers, suppliers, partners, contractors and anyone else associated with the enterprise. It should address information in all its forms.

2. Secure the "human element."

Humans are the single most important element of an information security program. Ultimately, all information dissemination is under their control. Security training and awareness, therefore, is essential. Employees need to be advised of threats, countermeasures and their responsibilities for safeguarding information. One biotech firm shows new employees a video of information thieves at work. The thieves swipe information from desks and computers and use social engineering techniques to get what they want. The video also outlines what employees can do to foil such attacks.

Non-disclosure agreements (NDAs) provide a mechanism for advising employees of their responsibilities. If an employee intentionally compromises secrets, the NDA provides grounds for termination or prosecution. Background checks can help identify persons who might compromise trade secrets before they are hired. Exit interviews can remind employees of their responsibilities when they leave.

3. Maintain physical security barriers.

Physical barriers, including locked gates, doors, safes, desks and filing cabinets, can be used to control physical access to information. Entry can be granted via guards, keys, badges, access tokens and biometrics. Biometrics technologies, including finger, iris, voice and face prints, are becoming increasingly attractive as users need not remember or carry anything. Prices for biometrics are falling and accuracy is improving.

Proper disposal of trash, including paper shredding, can keep sensitive information from outside "dumpster divers" as well as insiders who rummage through office trash bins. But keep in mind that paper shredders are not always foolproof, since documents sometimes can be reconstructed.

4. Update your electronic security tools.

Information must be protected both in storage and in transit over computer and telecommunications networks. This requires a combination of safeguards, including access controls, authentication, encryption and intrusion and misuse detection. Access controls—including computer and network login controls, firewalls and application-layer controls—prevent unauthorized access to information resources. Such controls can be applied to individual documents and records or to complete systems.

Authentication mechanisms validate the identity of users and other entities, including networked computers. Mechanisms include passwords, access tokens, biometrics, cryptography, digital signatures and location signatures. Without adequate authentication, access controls are useless, since cyber thieves can impersonate legitimate users and gain access to sensitive information.

Encryption, or the process of scrambling data into something that is unintelligible, can protect data transmitted over open computer networks and phone lines (fax and voice). Internet and LAN traffic is particularly vulnerable to eavesdroppers who deploy packet sniffers. Similarly, encryption can protect data stored on computers, which are vulnerable to physical theft and unauthorized access.

Intrusion and misuse detection systems operate on the principle that it is not feasible to prevent all attacks, particularly those by insiders, but that such attacks follow identifiable patterns or deviate from normal usage in identifiable ways. By monitoring system behavior, either from audit records or in real time, these systems attempt to detect intrusions by outsiders and misuse by authorized persons. Online systems may be integrated with other access controls and manual auditing procedures to detect and thwart penetration attempts.

Software tools that detect and eradicate viruses, worms and Trojan horses can be viewed as intrusion detectors applied to software. These tools scan for patterns in files,

e-mail attachments, and software downloaded from the Web.

Ideally, the above mechanisms are integrated together in a single system that provides policy and administrative support in addition to access control, encryption, authentication, and intrusion detection across an enterprise.

Intruders typically break into computers by exploiting known vulnerabilities in systems that are not properly configured or maintained. Corporations can protect against these attacks by scanning their systems for vulnerabilities and by penetration testing. Some companies use the same tools used by the attackers themselves, such as password crackers, war dialers and network scanners.

5. Adopt a strategy for contingency planning and incident handling.

The final step of an information security program is to plan for the worst—and then respond to incidents that arise. This includes taking out insurance policies and establishing procedures for handling incidents.