The Open Barn Door

U.S. firms face a wave of foreign espionage

BY DOUGLAS WALLER

It's tough enough these days for American companies to compete with their Pacific Rim rivals, even when the playing field is level. It's a lot tougher when your trade secrets are peddled by competitors. One Dallas computer maker, for example, recently spotted its sensitive pricing information in the bids of a South Korean rival. The firm hired a detective agency, Phoenix Investigations, which found an innocent-looking plastic box in a closet at its headquarters. Inside was a radio transmitter wired to a cable connected to a company fax machine. The bug had been secretly installed by a new worker—a mole planted by the Korean company. "American companies don't believe this kind of stuff can happen," says Phoenix president Richard Aznaran. "By the time they come to us the barn door is wide open."

Welcome to a world order where profits have replaced missiles as the currency of power. Industrial espionage isn't new, and it isn't always illegal, but as firms develop global reach, they are acquiring new vulnerability to economic espionage. In a survey by the American Society for Industrial Security last year, 37 percent of the 165 U.S. firms responding said they had been targets of spying. The increase has been so alarming that both the CIA and the FBI have beefed up their economic counterintelligence programs. The companies are mounting more aggressive safeguards, too. Kellogg Co. has halted public tours at its Battle Creek, Mich., facility because spies were slipping in to photograph equipment. Eastman Kodak Co. classifies documents, just like the government. Lotus Development Corp. screens cleaning crews that work at night. "As our computers become smaller, it's easier for someone to walk off with on says Lotus spokesperson Rebecca Seel.

To be sure, some U.S. firms have be guilty of espionage themselves—thou they tend not to practice it overseas, cause foreign companies have a tigh hold on their secrets. And American co panies now face an additional hazard: t professional spy services of foreign natio "We're finding intelligence organizatio from countries we've never looked at fore who are active in the U.S.," says t FBI's R. Patrick Watson. Foreign int ligence agencies traditionally thoug friendly to the United States "are trying plant moles in American high-tech comp nies [and] search the briefcases of Ame can businessmen traveling overseas warns CIA Director Robert Gates. Ad Noell Matchett, a former National Secu ty Agency official: "What we've got is th big black hole of espionage going on all ov the world and a naive set of American bus ness people being raped."

No one knows quite how much mo ey U.S. businesses lose to th black hole. Foreign go ernments refuse comment business intelligence they collect. The victims rarely publicize the espionage or report it to authorities for fear of exposing vulnerabilities to stockholders. But more than 30 companies and securit experts NEWSWEEK contacted claimed bi lions of dollars are lost annually from st len trade secrets and technology. Th week a House Judiciary subcommittee holding hearings to assess the damag IBM, which has been targeted by Frenc and Japanese intelligence operations, est mates $1 billion lost from economic espi nage and software piracy. IBM won't offe specifics but says that the espionage "run the gamut from items missing off loadin docks to people looking over other people' shoulders in airplanes."

Most brazen: France's intelligence ser ice, the Direction Générale de la Sécurit Extérieure (DGSE), has been the most bra zen about economic espionage, buggin seats of businessmen flying on airline and ransacking their hotel rooms for doc ments, say intelligence sources. Thre years ago the FBI delivered private pr tests to Paris after it discovered DGS agents trying to infiltrate Europea branch offices of IBM and Texas Instr ments to pass secrets to a French compet tor. The complaint fell on deaf ears. Th French intelligence budget was increase percent this year, to enable the hiring 1,000 new employees. A secret CIA repo recently warned of French agents roamin the United States looking for business s crets. Intelligence sources say the Frenc

ILLUSTRATIONS BY ROSS MacDONAL

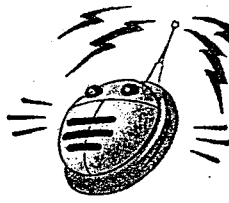
How the Spies Do It

MONEY TALKS

Corporate predators haven't exactly been shy about greasing a few palms. In some cases they glean information simply by bribing American employees. In others, they lure workers on the pretense of hiring them for an important job, only to spend the interview pumping them for information. If all else fails, the spies simply hire the employees away to get at their secrets, and chalk it all up to the cost of doing business.

STOP, LOOK, LISTEN

A wealth of intelligence is hidden in plain sight—right inside public records such as stockholder reports, newsletters, zoning applications and regulatory filings. Eavesdropping helps, too. Agents can listen to execs' airplane conversations from six seats away. Some sponsor conferences and invite engineers to present papers. Japanese businessmen are famous for vacuuming up handouts at conventions and snapping photos on plant tours.



BUGS

Electronic transmitters concealed inside ballpoint pens, pocket calculators and even wall paneling can broadcast conversations in sensitive meetings. Spies can have American firms' phone calls rerouted from the switching stations to agents listening in. Sometimes, they tap cables attached to fax machines.

HEARTBREAK HOTEL

Planning to leave your briefcase back at the hotel? The spooks will love you. One of their ploys is to sneak into an exec's room, copy documents and pilfer computer disks. Left your password sitting around? Now they have entree to your company's entire computer system.

Embassy in Washington has helped French engineers spy on the stealth technology used by American warplane manufacturers. "American businessmen who stay in Paris hotels should still assume that the contents of their briefcases will be photocopied," says security consultant Paul Joyal. DGSE officials won't comment.

The French are hardly alone in business spying. NSA officials suspect British intelligence of monitoring the overseas phone calls of American firms. Investigators who just broke up a kidnap ring run by former Argentine intelligence and police officials suspect the ring planted some 500 wiretaps on foreign businesses in Buenos Aires and fed the information to local firms. The Ackerman Group Inc., a Miami consulting firm that tracks espionage, recently warned clients about Egyptian intelligence agents who break into the hotel rooms of visiting execs with "distressing frequency."

How do the spies do it? Bugs and bribes are popular tools. During a security review of a U.S. manufacturer in Hong Kong, consultant Richard Heffernan discovered that someone had tampered with the firm's phone-switching equipment in a closet. He suspects that agents posing as maintenance men sneaked into the closet and reprogrammed the computer routing phone calls so someone outside the building—Heffernan never determined who—could listen in simply by punching access codes into his phone. Another example: after being outbid at the last minute by a Japanese competitor, a Midwestern heavy manufacturer hired Parvus Co., a Maryland security firm made up mostly of former CIA and NSA operatives. Parvus investigators found that the Japanese firm had recruited one of the manufacturer's midlevel managers with a drug habit to pass along confidential bidding information.

Actually, many foreign intelligence operations are legal. "The science and technology in this country is theirs for the taking so they don't even have to steal it," says Michael Sekora of Technology Strategic Planning, Inc. Take company newsletters, which are a good source of quota data. With such information in hand, a top agent can piece together production rates. American universities are wide open, too: Japanese engineers posing as students feed back to their home offices information on school research projects. "Watch a Japanese tour team coming through a plant or convention," says Robert Burke with Monsanto Co. "They video everything and pick up every sheet of paper."

Computer power: In the old days a business spy visited a bar near a plant to find loose-lipped employees. Now all he needs is a computer, modem and phone. There are some 10,000 computer bulletin boards in the United States—informal electronic networks that hackers, engineers, scien-

tists and government bureaucrats set up with their PCs to share business gossip, the latest research on aircraft engines, even private White House phone numbers.

An agent compiles a list of key words for the technology he wants, which trigger responses from bulletin boards. Then, posing as a student wanting information, he dials from his computer the bulletin boards in a city where the business is located and "finds a Ph.D. who wants to show off," says Thomas Sobczak of Application Configured Computers, Inc. Sobczak once discovered a European agent using a fake name who posed questions about submarine engines to a bulletin board near Groton, Conn. The same questions, asked under a different hacker's name, appeared on bulletin boards in Charleston, S.C., and Bremerton, Wash. Navy submarines are built or based at all three cities.

Using information from phone intercepts, the NSA occasionally tips off U.S. firms hit by foreign spying. In fact, Director Gates has promised he'll do more to protect firms from agents abroad by warning them of hostile penetrations. The FBI has expanded its economic counterintelligence program. The State Department also has begun a pilot program with 50 Fortune 500 companies to allow their execs traveling abroad to carry the same portable secure phones that U.S. officials use.

But U.S. agencies are still groping for a way to join the business spy war. The FBI doesn't want companies to have top-of-the-line encryption devices for fear the bureau won't be able to break their codes to tap phone calls in criminal investigations. And the CIA is moving cautiously because many of the foreign intelligence services "against whom you're going to need the most protection tend to be its closest friends," says former CIA official George Carver. Even American firms are leery of becoming too cozy with their government's agents. But with more foreign spies coming in for the cash, American companies must do more to protect their secrets. ■

Seeing Public Service as an Investment

Arnold Hiatt believes Ivan Boesky had it half right. "He said greed is good, but he should have continued, 'Enlightened self-interest is better'." While many corporate chieftains slash costs and cut staffs, the 64-year-old chairman of Stride Rite Corp. is spreading a little enlightenment of his own. The Cambridge, Mass., footwear marketer earmarks 5 percent of pretax earnings for the Stride Rite Foundation, its philanthropic arm. In 1991, the group funded projects ranging from intergenerational day care to inner-city education. Last week, after stepping down as chairman to devote full time to the foundation, he talked with NEWSWEEK's Annetta Miller.

How can you pay for social programs when other companies say times are too tough?

There is nothing unique about Stride Rite. We have shareholders looking for the same return on their investment as any other public company. We're different only to the extent that we've gone beyond the traditional limits of how we define our social responsibility. We look at public service as an investment. We believe the well-being of a company cannot be separated from the well-being of the community. If we're not providing the community with access to day care and elder care, if we're not providing proper funding for education, then we're not investing properly in our business.

Aren't your programs costly?

It costs infinitely less to spend money on initiatives such as the ones we sponsor than to, say, pay the costs associated with a young child who hasn't had a good head start and ends up in a prison or detention center. Take our family-leave policy. It costs us next to nothing. And yet the statement it makes to employees is powerful. It says to them that we care. And when employees know you care about them, they tend to be more productive. It's the same with our day-care center. To me, it's a no-brainer. But it's the kind of thinking that seems to elude the Oval Office.

Is there a link between corporate responsibility and profits?

A recent study by the Covenant Investment Management in Chicago found that responsible companies tend to produce a higher return to stockholders. They explained this in terms of "stronger employee and community relations, customer loyalty and less regulatory interference." My additional explanation has to do with the greater sensitivity of management. If you develop a certain acuity in listening to consumers, you also learn to listen well to your employees and to the community. Have our stockholders suffered? Well, those that invested $10,000 in 1984 would now have $155,000. Not bad.

What are your plans for the foundation?

One of the things I'm intrigued with is volunteerism. That is to me the noblest calling of all. And yet, while we in the corporate world are given far too much in compensation, people in public service are often not recognized financially. One of the things we do at Stride Rite is to pay our employees to do mentoring in inner-city schools for two hours a week. It creates energy, good will and a hope of making a difference. But maybe the biggest contribution we can make as a foundation is using our voice to reach our partners in government. We must help our political leaders to understand the difference between a "free market" that allows the Keatings of the world to loot S&Ls and "competitive market forces" that are thoughtfully controlled so that greed and enlightened self-interest are distinguished. If the politicians want to be pro-business, we must educate them on the business of business.

Little feet: *Hiatt and friends at a company-funded day-care center*
DAVID RYAN—BOSTON GLOBE