

Mission Possible

Industrial Espionage Getting More Common and More Crucial

By Andrew Chang



Dec. 4 — For a good part of his professional career, Andrew Parsons has been a computer software sales executive. But when he received an e-mail from an anonymous person earlier this year, he took on a more exciting role — he became an undercover agent for the FBI.

The e-mail Parsons received was from a disgruntled employee of Atlanta-area computer firm NetSupport, a rival to his employer at the time, Vector Networks — offering to sell him their complete customer database for \$20,000.

Parsons decided to react by notifying NetSupport's CEO, and not long after, the FBI contacted him. The bureau asked Parsons to participate in a sting operation, and he agreed.

Parsons arranged to meet the seller at a local hotel, and arrived with a suitcase full of cash.

In an internal company memo, he recalled the meeting: "I was nervous, because I didn't know if he was armed. And I was also surprised to find that he did not come alone — there was another fellow with him."

But the FBI was also waiting in an adjoining room, equipped with monitors, microphones, and recording equipment. Once the transaction had been made, they burst into the room and arrested the two men.

The disgruntled employee was charged in a federal case and pleaded guilty some weeks after he was caught, said Dave Auwarter, CEO of NetSupport. His sidekick did not work for the company. The FBI "nailed them in many different ways," he said.

Parsons has since left the company, but the memory of his adventure is still fresh in the minds of his former employer. "I was shocked to learn about the bribery incident from Andy, and was even more surprised to learn of his agreement to assist the FBI. I truly believe that Andy is a hero," said Vector Networks press officer Judith Drucker.

And while Parsons is unusual for the gamble he took, the type of deal he was offered is getting to be par for the course in today's commerce-driven world, experts say.

Some security experts say instances of industrial espionage are getting more common — even as industrial security is becoming more important.

Dual Threats

Technology is making it easier for thieves to copy, transfer and sell information, said Tom Patterson, head of security services in Europe, the Middle East, and Africa for global professional services firm Deloitte & Touche.

You used to have to be inside the company to get access, Patterson said. Today, he said, "you get a \$200 CD burner, and you get the whole works." Parson's seller, for example, would have found it much harder to make his offer without a computerized database and an anonymous e-mail account.

Meanwhile, governments around the world are learning that security breaches at certain companies may pose threats to national security. Last month, Sweden expelled two Russian diplomats in connection with an espionage case at cell phone maker Ericsson.

Ericsson is also developing radar and missile guidance systems for a Swedish warplane — one of three planes competing for a \$3.5 billion Polish contract.

"Taking down a banking network in a country, transportation networks, oil networks, those designated critical infrastructures — people who threaten those industries are threatening national security," Patterson said.

"It's on the same plane as taking down a jet fighter as a bank network."

Enormous Damage

A September 2002 report by the American Society for Industrial Security found that 40 percent of the companies participating in its survey reported incidents of known or suspected losses of proprietary information between July 2000 and June 2001.

The study also found that as much as \$400,000 was lost on average per incident. An earlier ASIS study estimated that the damage caused by economic or commercial espionage to American industry in a single year, 1997, was \$300 billion.

However, experts are quick to point out that these figures are largely estimates — because many companies are reluctant to reveal they were victims of espionage, and because many cases of espionage went undetected.

"The perpetrators keep quiet for obvious reasons. The victims do so out of fear," Frank Ciluffo, deputy director of the CSIS Global Organized Crime Project said in his address to the World Economic Forum in 1998.

"It may jeopardize shareholder and consumer confidence. Employees may lose their jobs. It may invite copycats by inadvertently revealing vulnerabilities. And competitors may take advantage of the negative publicity."

A Tricky Business

And still more industrial espionage cases are stifled or turn out to be misdirected. Trade secrets and intellectual property are complicated issues to sort out, and few cases have willing witnesses like Andrew Parsons.

In one of the more recent cases of international industrial espionage in the United States, two Harvard researchers were arrested in June, accused of stealing lab equipment and trying to sell trade secrets that belonged to Harvard to a Japanese drug firm.

Harvard says the two signed routine agreements that gave it the right to any discoveries made in the lab where they worked. The pair say they were only trying to further their research, and are free on bail.

Prosecutors have hinted that they are exploring the prospect of a settlement rather than try an expensive case involving complex issues.

In another recent case, authorities arrested Han Bin, a Chinese-born researcher at the University of California, Davis, after finding 20 vials of biological samples in his home refrigerator, and a plane ticket to China — days after he had been fired.

But after less than a month, most charges against the researcher were downgraded or dropped. Han said the vials were in his freezer to save a trip to the lab, and the ticket turned out to be round-trip, for a long-planned visit to see his parents.

Experts say industrial espionage is especially hard to prove in the academic world, mainly because it is loathe to put controls on information. The most publicized case of alleged espionage in recent years, against Taiwanese-born scientist Wen Ho Lee, fell apart on similar grounds.

The government accused Lee, a researcher at the federal laboratories at Los Alamos, N.M., of copying nuclear secrets and passing them to the Chinese.

Lee said he had made the copies to work at home. He was largely exonerated.

Dipping Ties, Sticky Suitcases

Outside of the academic world, information is more closely guarded, but instances of industrial espionage have still been hard to prove.

According to former U.S. intelligence officer John Nolan, 60 percent of U.S. firms have "competitive intelligence" divisions — which investigate rivals mainly through legal means.

Nolan currently operates the Centre for Operational Business Intelligence, which teaches businessmen and women how to use the intelligence techniques Nolan once used to serve the country, to serve corporate ends.

"You identify people, their positions and their ability to provide information, wittingly or unwittingly," he said — sometimes as simply as asking calling and asking questions and approaching people at trade shows.

It's a matter of assessing people, finding out what's going to make them a cooperative source of information, he said. Many people are 'frustrated teachers' who enjoy explaining the complexity of their work, he said.

"But people also respond to flattery, criticism, disbelief, challenge — there's a variety of elicitation techniques," Nolan said. He is quick to point out that everything he does is legal.

But the annals of corporate espionage also contain tales of more exotic and legally questionable exploits.

Experts recall spies going on company tours with small cameras hidden in pens and visitors "accidentally" dipping their clothes in vats of secret chemicals or using briefcases and shoes with sticky bottoms to pick up clues from factory floors.

One of the most fantastic gambits took place in 1988, when a team from France's General Directorate for External Security, the intelligence arm of the French ministry of defense, traveled to the United States to spy on the development of the new Boeing 747-400.

The team set up in a house in Washington state, near where Boeing was doing its test, and with the help of insiders, retrieved test data that was being beamed to another facility. The data was later passed on to Toulouse-based Airbus for incorporation into its Airbus 340.

The former chief of the DSGE admitted to the action eight years later in 1996 on a German TV special. "All secret services of the big democracies undertake economic espionage," he said.

All U.S. intelligence agencies deny being involved in industrial espionage.

A Continuing Problem

Congress only made industrial espionage a federal crime six years ago, when it passed the Economic Espionage Act in 1996.

Before that, industrial espionage cases could only be prosecuted in state court, which weren't prepared to deal with the big cases that involve foreign governments or multinationals.

But in a sign of how rare such cases are, Justice Department records show there have only been 36 prosecutions under the EEA so far. Of those cases, half were filed since 2000.

Trade secrets, which are protected by the EEA are notoriously difficult to protect. Trade secret protection is basically a tautology — it lasts for as long as the secret is kept confidential.

Once a trade secret is made available to the public, trade secret protection ends.

As difficult as industrial espionage cases are though, experts said they are important — even in this era where terror concerns trump all others.

Nolan pointed to how investigators discovered, in the wake of 9/11, certain Islamic religious charities had been infiltrated and taken over by individuals linked to terrorists.

The same could happen to companies, he said, noting "lifeblood is money." ASIS directors met with the Department of Homeland Security last month, kicking off what ASIS personnel said they expected would be a permanent relationship between the organizations.

Terror notwithstanding, the layman should be concerned about industrial espionage simply because so many companies are now publicly-held.

And any blow to their bottom line is a blow not only to the economy, but potentially to the wallets of individuals. With every instance of industrial espionage, Nolan said, consumers should be asking: "Are they doing what they can to protect my investment?"

"If we're living in an information society, information has value. If you don't protect that information, you're going to wind up losing that value," Nolan said. ■