INDUSTRIAL ESPIONAGE CASE 1 -- TAKING OVER WHERE COLD WAR SPYING LEFT OFF

Companies aren't just spying on rivals, they're also getting the skinny on clients, potential partners.

By Peter Benesh (Investor's Business Daily)

The end of the Cold War put a lot of spies out of work. Many are finding new jobs in the booming field of corporate espionage.

Case in point: The British counterspies at MI5 are investigating France's spy agency, the Direction Generale de la Securite Exterieure. It seems a DGSE agent sent back secret data from three U.K. firms for which he'd worked. The DGSE handed the informtion to grateful French companies. Extraordinaire? Au contraire; it's happening more and more, experts say. Governments often help their hometown industries. But spying is also a business-to-business pursuit. Just four months ago, software giant Oracle got caught buying trash - Microsoft trash. It had hired a firm to dive in the Dumpsters of trade groups friendly to Microsoft. "Trashint" - trash intelligence - is just one technique. Bribing insiders for company secrets is another.

The trade term for corporate espionage is competitive intelligence. To fight it, Congress passed the Economic Espionage Act, which took effect Oct. 11, 1996. With the FBI in charge of investigations, the act hits spies who steal secrets for foreign interests or economic gain.

"Neither the FBI nor the U.S. intelligence community. has. evaluated the costs of economic espionage," Sheila Horan, FBI deputy assistant director, told Congress last month.

An Expensive Game

Damage to Fortune 1000 companies could be as high as $250 billion a year, said Richard Heffernan, whose firm, R.P. Heffernan Associates Inc. of Branford, Conn., protects intellectual property. "Competitive intelligence gathering is a gray area," Heffernan said. "Many methods are legal. But eavesdropping and trash-searching at executives' homes are illegal." One scam he's seen is the phony job interview; a firm will lure a rival's workers to apply for nonexistent jobs, just to elicit trade secrets.

Darryl Thibault, president of PeXis Corp., a San Diego security firm, said the Internet is a great source. But it's not all fair game. "Even data online, such as driving and credit records, could be illegal," warned Thibault, a former CIA base chief in Europe.

Not all spying is aimed at trade secrets. Thibault called the Oracle-Microsoft case "a beautiful example of the level of sophistication that competitive intelligence has reached." Oracle wanted to help the government's antitrust case against Microsoft, he noted. "Microsoft was on the mat, and Oracle hired investigators to get information the government was not digging up. Oracle stood to benefit by adding to Microsoft's troubles."

Spy On Both Sides

Another aim of corporate espionage is to get the plans of rivals, or even potential partners. When millions or billions of dollars are at stake, "You have to know the intentions of your business ally or client," said Leonard Holtzworth, president of Laguna Beach, Calif.-based International Program Group. "You must know if they're double-dealing**. Business espionage is more ruthless than government spying."** When nations spy on each other, "They have strategic goals that may not be realized for years," Holtzworth said. But business is focused on "getting the deal and making the profit." Business espionage is tactical, with "specific retrieval goals," while government spies may be on fishing expeditions.

Security experts agree that carelessness leads to huge data losses. Qualcomm Chairman Irwin Jacobs "raised the bar," Heffernan said, when his laptop computer disappeared. Stolen from a hotel lectern in Irvine, Calif., last month, it held many company secrets.

Corporate executives are not alone in breaching common-sense security rules. U.S. State Department and U.K. Defense Ministry officers have lost top-secret laptops, too. **British spy and defense agents lost 67 laptops in the past three years. The State Department admitted that it lost 15 from 1999 to mid-2000.** Loss is epidemic in the private sector. "I can't tell you the number of people I've heard of who travel the New Haven Railroad and put their laptops on the overhead bin and take a snooze. When they wake up, there's no laptop," Heffernan said.

Shareholders and the public don't hear of those losses or of most of the data thefts or leaks from companies, said Ira Winkler, author of the book "Corporate Espionage." Much data theft is low-tech, he says. He describes one ploy as the thief dressed as a courier who gets access to inner offices. "All you have to do is have the nerve to get away with it," he said.

Silent Victims

When a company discovers it's been hit, Holzworth said, "it wants to lose the problem as quietly as it can. Companies don't want to be seen as negligent." **"Publicity can adversely affect stock prices, customer confidence and ultimately competitiveness and market share,"** the FBI's Horan said.

"The future of intelligence is in the private sector," Thibault said. "I ran into a former KGB officer at a conference. He had spent his career stealing secrets from U.S. aerospace companies. Now he's marketing his services to the same industry." As well, there's "an explosion of technology available." At the airport in Zurich, Switzerland, you can buy just about any spy gear you want, Thibault says.

Governments nurture business spying against allies. "There are no friendships in corporate espionage," Thibault said. A U.S. company with a French office is going to be bugged, he says. Other allies that help industry spying are Taiwan, South Korea and Germany. China's espionage is renowned.

Even Britain is in the game. In July, a new law let U.K. agents sift through all e-mail. The law threatens a two-year jail term for withholding encryption codes, but the government says corporations may submit printouts of messages.

No country is above suspicion. Some EU countries claim that the U.S.-run Echelon monitoring system is spying on European business for economic advantage. A French prosecutor is investigating.