

Economic/Industrial Espionage

by Ben N. Venzke

The days when spy vs. spy meant the CIA vs. KGB are no longer. In this day and age of corporate espionage it all too often means French intelligence against IBM, or even Mitsubishi against Ford Motor Company. Economic and industrial espionage is being carried out around the world and US companies are prime targets, not to mention easy ones.

US companies have remained blissfully unaware of corporate espionage practices for some time. Unless a company worked as a defense contractor, there was no reason to worry about "spies." But France, Japan and several other countries have been at it for decades, and now the threat posed by economic and industrial espionage is beginning to be taken seriously by US executives.

In Japan the underlying philosophy is, why spend 10 years and \$1 billion on research and development when you can bribe a competitor's engineer for \$1 million and get the same, if not better, results. In France, the philosophy is that while France and the US may be military allies, we're economic competitors. Meanwhile, South Korea recently intensified efforts to collect information from foreign companies for South Korean corporations _ a fact discussed openly on South Korean television.

Even Russia is getting on the industrial espionage bandwagon. President Boris Yeltsin three months ago ordered top Russian officials to "close the technology gap with the West and told them to make better use of industrial intelligence to do so," according to Senate Select Committee on Intelligence Chairman Sen. Arlen Specter, who spoke at a recent hearing on the issue.

The potential losses for all American industry could amount to as much as \$63 billion, according to a study by the American Society for Industrial Security. The actual dollar amount is heavily debated, but very few would argue it isn't significant. Taken in light of Secretary of State Warren Christopher's recent comment at a Capitol Hill hearing that "our national security is inseparable from our economic security," the problem can't be taken lightly.

The FBI has taken the lead role in what is a relatively new campaign to stop economic espionage. The bureau is currently investigating allegations of economic espionage activities against the US by individuals and organizations from 23 different countries. Even local FBI offices _ including the one in Boston _ are helping in the campaign to protect the nation's trade secrets.

Corporate America has been especially vulnerable to economic and industrial espionage because it lived a rather sheltered life from what is considered in many countries to be an acceptable way of doing business. But as more and more US corporations see their secret marketing plans and research and development work stolen for a mere fraction of what it cost them, they are beginning to realize the gravity of the threat. Words such as penetration, mole, hacker, and spy are slowly being added to the corporate lexicon of senior executives. And Congress is now considering legislation that would make easier the prosecution of those who perpetrate economic espionage.

Those "spies" employ a variety of methods _ some legal, some not _ to steal a company's secrets, or collect information. One of the most valuable and damaging methods is to recruit an agent inside the target company by either bribing or blackmailing an employee. Foreign governments have also been known to allow students to study abroad and take internships in target companies as an alternative to compulsory military service. Once these students graduate they are frequently urged to take jobs at the companies they interned with, thus providing them with a constant supply of information.

International exchange organizations, friendship societies, import-export companies, and other such organizations are frequently used by foreign governments in order to get close to certain companies. "These organizations spot and assess potential foreign intelligence recruits with whom they have contact," said FBI director Louis Freeh.

Companies will also use legitimate business agreements, such as licensing and on-site liaison officers, to provide opportunities to gather information illicitly. One such case involved Recon Optical. The company signed a 4-year, \$40 million contract with a foreign government to design an airborne surveillance camera. The terms of the contract allowed three foreign Air Force officers to work in Recon's company plant. After continual cost disputes and other problems, Recon canceled the contract and dismissed the three officers. As the officers were leaving, security guards at the plant caught them removing boxes of company documents. It turned out that during the officers' stay they had been passing information to their government-owned defense company. The documents enabled the company to build its own system without Recon Optical.

An even more complicated problem for law enforcement is the growing use of offshore hackers to break into US corporations' computer systems and steal trade secrets. The fact that the attack can come from outside the US makes an already difficult prosecution next to impossible. In some cases the hackers are even backed by the countries they're working from. Not all the methods are so high-tech or filled with spy tradecraft. Some simple, if rather bold, ways have proved just as damaging. Raymond Damadian, president and CEO of Fonar Corp., said "To protect the technology of our magnets (used in MRI machines), which was precious to the company, we required that all of our magnet installations take place behind locked doors. A Siemens executive proudly told me that that precaution was easily overcome. He reported that he took the technician out to dinner, filled him with alcoholic beverages and thereby secured an invitation to enter the room and inspect the scanner for as long as he wished, which he did."

Legal methods such as Freedom of Information Act requests are also a vulnerable point for US corporations. When Mitsubishi decided in 1986 to enter the space industry it began an intensive effort to gather information. FOIA requests became a major resource because they allowed the company to get information from NASA. According to some estimates, Mitsubishi filed over 1,500 requests in 1987 alone.

The US Patent Office is another weak point. "The Japanese and others spend a great deal of time in the US patent office, which is considerate enough to provide free copies of all US patents," said National Intellectual Property Law Institute President James Chandler.

According to Dan Whiteman, the corporate information security officer for General Motors Corporation, "Unfortunately, no matter how elaborate the precautions taken, it is nearly impossible to stop economic espionage when the rewards of wrongful conduct are so high _ and the perceived risks of being held accountable are so low."

The low level of accountability that Whiteman refers to reflects a lack of effective laws.

"The FBI has attempted to use various criminal statutes currently in force to counter economic espionage, but these laws do not specifically cover the theft or improper transfer of proprietary information, and therefore are insufficient to protect these types of items," said Freeh.

"In several instances, the FBI has conducted investigations only to have prosecutions or permission to use further investigative procedures declined by Federal prosecutors because of lack of statutory criminal predicate."

Another problem facing the prosecution of cases dealing with economic espionage is that the confidential information stolen is commonly made public during the hearing. "Proprietary economic information derives value from its confidentiality; if this is lost during legal proceedings, then the value of the information is greatly lessened," said Sen. Specter.

Thomas Brunner from the US Chamber of Commerce said, "It may well be the ironic consequence of our legal rules that in order to obtain justice the victim of economic espionage will have to make public the very information whose theft it is complaining about." He even adds that, ". . . it is at least theoretically possible that where the US Attorney is determined to pursue a prosecution, the victim could be forced to make such a disclosure even when it did not actively request the enforcement action."

The FBI, however, is making a lot of progress in dealing with awareness through its DECA _ short for Development of Espionage, Counterintelligence, and Counterterrorism Awareness _ program. The program works to enhance corporate security directors' awareness to the threat and helps them to counter it. The most recent addition to the DECA program is DECA Fax. The new service faxes unclassified counterintelligence information to companies who fear they are targets of espionage. The information in the fax is designed to help them spot the perpetrators, revealing, for example, the methods or guise used by "spies" known to be in circulation. Boston's FBI office has recently begun the program for corporations in the area.

In response to the legal problems facing agencies charged with combating economic and industrial espionage, Sen. Specter and Sen. Kohl have introduced the "Industrial Espionage Act of 1996" in Congress to help prohibit economic espionage and protect proprietary information. If passed, the bill will go a long way in establishing a basis for prosecution in economic espionage cases.

(C) 1996 Ben Venzke, who is based in Boston and the publisher of the Intelligence Watch Report.