How Foreign Spies Get U.S. Firms' Secrets

BY DON CLARK
Chronicle Staff Writer

Foreign spies are stealing secrets from U.S. companies, and the government doesn't intend to take it anymore.

"We know that foreign intelligence services plant moles in our high-tech companies," said Robert Gates, Central Intelligence Agency director, during his confirmation hearings in September. "We know that they rifle briefcases of our businessmen who travel in their countries.

"We know that they collect information on what we are doing, and I think the CIA and FBI working together should have a very aggressive program against it."

That requires a big change in mindset for the two agencies, which are used to collaborating against Soviet-bloc spies seeking military and intelligence secrets. The FBI is now trying to get a handle on the problem of other spy services working against companies in the Bay Area.

"We've talked to a lot of the corporations in the Silicon Valley about what they've observed," said Patrick Watson, FBI deputy assistant director, in an interview.

Watson, who ran FBI counterintelligence in San Francisco before moving to Washington, said the office has long worried about spies taking classified technology from local defense contractors. For the first time, he said, the FBI is also worrying about the theft of unclassified commercial technology that is "critical to the economic well-being of the United States."

Spies work in two basic ways. They plant informants inside an organization, or they use high-tech devices to bug offices and intercept communications.

American companies have encountered both. French intelligence agents, for example, have allegedly received sensitive information from French employees of IBM and Texas Instruments Inc. and passed it to the government-owned computer company Groupe Bull.

Eavesdropping is tougher to detect, and anecdotes hard to find. But Watson says U.S. companies should beware that their phone calls, fax messages and other electronic communications can often be picked up by foreign embassies and consulates in this country. And travelers should realize that government agents in some other countries work with companies and government-owned phone utilities to eavesdrop on American executives.

"They call up the phone company and say, 'Let us know this senior vice president's faxes and his telephone conversations and his computer accesses,'" said Noel Matchett, a former National Security Agency official who heads Information Security Inc. in Silver Spring, Md.

When the executive phones home or sends messages with a laptop computer, he said, eavesdroppers can pick up security codes needed to roam through company databases or voicemail systems.

Japan, America's biggest economic rival, is rarely accused of such subterfuge. But its government still picks up voluminous information about U.S. technologies and markets, through informal data-sharing relationships with Japanese manufacturers and trading companies, their U.S. subsidiaries and Japanese students at American universities. The flow of information toward Japan has increased as Silicon Valley companies turn to Japanese investors when they can't find traditional venture capital.

"For all intents and purposes, a company's technology transfers to Japan the same day the investment is made," said one Silicon Valley entrepreneur who has worked for Japanese and U.S. semiconductor companies.

U.S. companies are tightening up. They are hiring guards, installing electronic alarm systems and drilling employees in information security policies. Hot items include cellular phones and fax machine that uses a technology called data encryption to scramble information so faxes can't be read by outsiders.

As more companies use computers to swap sensitive documents, similar encryption techniques are becoming the norm on public data networks. The catch: NSA, America's eavesdropping agency, has fought use of the most advanced security technologies because they make its job harder.

SF Chronicle
2/18/99