

# **Industrial Espionage**

## **The Secret Agents of Fortune**

**by Mike Consol - The Business Journal**

If you don't spend much time fretting about corporate espionage, you may want to introduce a little paranoia into your life.

To hear Michael Anderson tell it, the times may never have been so ripe for high-stakes corporate espionage. Then again, Anderson gets paid to be paranoid. He is president of New Technologies Inc., a Gresham company specializing in forensic and computer security software programs. Anderson also spent 25 years as a gun-toting special agent with the U.S. Treasury Department.

Consider the potential for corporate espionage is so vast two years ago the FBI and CIA told U.S. business it was on its own. The federal agencies admitted there was no way it could protect American business from itself or foreign agents.

If you're ready to pay attention, know this: The enemy most often lies within, says Anderson. About 85 percent of espionage crimes are perpetrated by employees. Your intranet firewalls may be great at keeping outsiders out, but do nothing to prevent insiders from turning into outlaws by exporting company secrets.

Let's start with those Y2K programmers you have brought in house. Did you conduct background checks? Or do you feel lucky just having found a team of supposedly qualified software pros.

Consider their potential for mischief. Besides having immediate access to the reservoir of company information, unscrupulous programmers could plant a Trojan horse in a corporate computer system. In other words, build a secret "backdoor" affording them repeated access to company data. Depending on your company's rank in life, that data could fetch huge sums of money.

Also beware the duplicitous executive or systems information person who will use Y2K-day as a decoy while heisting millions in cash or company information.

The high-ranking executive on the road with a laptop computer is another extreme vulnerability, says Anderson. The laptop is no doubt loaded with the company's latest and most vital activities. Typically, laptops are left in the hotel rooms during the dinner hour. A good spy need simply to pop into the room when the maid is turning down the bed and pretend it's his room. It's a rare maid who would even begin to challenge such an interloper.

Once inside, the spy can boot-up the laptop, copy all data contained on the hard drive and leave the room without a clue that high crimes and misdemeanors have been committed. A partner in crime with a cellular phone may be staking out the executive's restaurant of choice to ensure the mission can be aborted if dinner is unexpectedly cut short.

Anderson, who sits on the advisory board of the National White Collar Crime Center, carries a laptop while on the road, but has its data protected by 128-bit encryption technology, making its theft a virtual impossibility.

You may not be much safer while aboard an airliner. Anderson says the French have been accused of bugging seats in the first-class section of their airliners. Ditto for French hotel rooms frequented by executives. In addition to France, Japan and Israel have been cited as nations active in the corporate espionage business.

Economic prosperity, after all, is a matter of national security. Companies may turn on one another because billion-dollar technological chasms can be closed quickly and relatively cheaply with a spy mission or two.

Among the saboteurs believed to be posing threats to business are former agents of the Soviet Union's dreaded KGB. They found themselves looking for new employ after the Cold War lost its chill.

The business world has become more vulnerable than ever to espionage, says Anderson, because its information has moved from paper to computer.

"Computers were never intended to be secure," he says. "If you can get your hands on the keyboard you can get information out of the computer."

There are ways to protect yourself, Anderson says.

- Lock your doors. Computer passwords alone won't keep determined infiltrators from stealing.
- Encrypt sensitive computer files.
- Shred all paper documents before trashing them.
- Don't discuss company secrets in unsecured environments.
- Don't assume your consultants and temps are working on your behalf.
- Some well-placed paranoia could save your company from financial calamity and public humiliation.