

include anything from having employees sign confidentiality agreements to making sure basic security is in place so even the smallest bit of information isn't scooped up by rivals.

Local investigator **Wayne Black**, who investigates corporate spying claims, added that all companies at one time or another have been victims of a security breach.

But he said in his experience as an investigator, being prepared is essential for companies.

"It's kind of like wearing a seat belt," Black said. "I'm probably not going to get into an accident today, but what if?"

## Start with a list

Getting started is the hardest part.

First, officials should write down the company's proprietary information, suggested **Milton Ferrell, of the law firm Ferrell Schultz Carter Zumpano & Fertel**, a Miami-based attorney who represents companies that have been victims of corporate spying. That information includes what products and employee resources are considered classified.

Officials should require all employees to sign a written policy that makes clear what they should not talk about. Also, the policy should state that lists of clients are proprietary and not to be taken should an employee quit or be fired.

"You don't want to start by spending a lot of money; you want to start with your employees," Ferrell said.

Company officials should also make it clear to employees that any information on business computers is not confidential.

"Companies need to communicate to the employees that the system is owned by the company and there is no expectation of privacy," Black said.

Ferrell also advises companies to conduct background inspections, including credit and criminal checks and drug screenings, before hiring an employee and throughout his tenure. And references should be checked.

## Protect the buildings

After officials secure their work force, the next step is to safeguard their buildings, including the actual office and the information installed on computers.

Black, the local investigator, said many times companies think their buildings are secure, when in fact they're not. When a business hires Black, he will try to gain access to the building. He will walk into the office unannounced and say he's there to back up the computer system. Nine times out of 10, he said, the receptionist will send him back to the computer area.

If questioned in the computer support area, he will say something about misreading the company's address. Then he'll pop out the disk he was using to copy data files off the main server and walk out. Usually, he's not stopped or questioned.

Ferrell suggested companies also use identification cards programmed to allow employees access only to areas where they need to be. In a law office, for exam-

ple, not all employees need to enter rooms where case information is being stored.

As more information is kept on computer hard drives, companies need to be watchful of hackers entering their buildings through communications cables.

Those in the industry suggest installing firewalls and anti-virus software, as well as anti-hacking software. But others say that while those protections are needed, a spy hacking into a computer system is not much of a threat.

"That's really not as big an issue as a lot of people believe it is," said Steve Ackerman, director of research and analysis at **CTC International Group** - a West Palm Beach-based firm that tries to obtain secrets for companies. "The real problem is an employee inside the company that has access and downloads that information and is willing to forward that information to someone else for money," he said.

Next, companies need to watch what is being thrown in their trash. Once trash lands in the dumpster, it's considered abandoned.

"If you want something to be secret you better treat it like a secret," said **William Richey**, a Miami attorney who also works with clients who have been victims of corporate spying.

## Make it confetti

While many companies shred their documents it's usually only done in strips, which can be easily pieced together. Black suggests getting a shredder that cross-cuts, making the paper almost like confetti.

Companies even can hire businesses to pick up and shred their documents on site. **Shred-It**, which has offices in Dania, has seen its business grow by about 60 percent each year. The company charges about \$3.85 a minute and its shredders can cut through more than 1,200 pounds of paper an hour.

"In today's society, people are becoming more aware of their vulnerability. There's a heightened awareness because of things that have happened," said Ron Ofiara, the company's general manager.

Shred-It provides businesses with a locked cabinet where they can put sensitive documents that need to be shredded. The documents fall into a sack similar to a laundry bag. Only one person in the office has a key to the cabinet, Ofiara said.

A Shred-It driver then comes and opens the cabinet, zips up the bag and carries it to the truck. The information is then fed into a high-speed shredder and the company receives a receipt detailing the time and location, Ofiara said.

While companies may find many of these suggestions expensive, those in the industry say if the information is worth protecting, businesses should do whatever they can to keep the secrets from falling into the wrong hands.

"It's no different than spending \$35 for a lock on your door," Black said. "Pay now or pay later."