



AT THE BAR

I got a panicked call last week from a client who had just laid off one of his senior managers. New to this heart-wrenching process, this CEO had spent weeks running the numbers and hammering out what he thought would be a fair severance package. He had drafted his announcement to the staff and mapped out a transition scenario. He had scripted, rehearsed, and re-rehearsed the termination interview. He had carefully timed the interview, which, while painful, had gone essentially according to plan.

Believing that he had handled the termination as well as he could, my client finally was able to get a full night's sleep. But while driving to work the following morning, my client realized that there was one very important thing that he had missed: he had done nothing to secure the highly confidential and valuable company information to which his former manager had had free access, information that could cause my client irreparable harm were it to fall into the wrong hands.

In the world of intellectual property law, confidential information that provides a company with an advantage over its competitors is protectable as a "trade secret." Trade secrets can take many different shapes and forms, from manufacturing know-how to coveted customer lists, favorable contract terms to yet-to-be launched marketing and branding strategies, sensitive financial information to acquisition or merger plans. A trade secret can be as sophisticated as a chemical formula for a new production catalyst or

Keeping Secrets

Securing the crown jewels in a down economy

BY LUCY PRASHKER

as simple as a recipe for a five-star restaurant's signature fruit salad. Indeed, while often considered the poor cousin of other intellectual property rights in trademarks, copyrights, and patents, a company's trade secrets can often be among its most valuable assets, representing the "crown jewels" of the enterprise.

Where there are jewels, there is temptation, and the more valuable the jewels, the greater the temptation. Add exiting employees to the mix, and temptation can quickly turn to information theft. Recent statistics are quite alarming. One survey published earlier this year revealed that 59 percent of workers laid off during the prior twelve months admitted to having left with corporate information, including e-mail lists, financial and non-financial business information, customer lists, and employee records. In a second recent survey, a whopping 88 percent of IT professionals, when asked, said that if fired tomorrow, they would take corporate information with them. Scary stuff.

What can be done? We advise our clients to follow a five-step plan. First, you've got to identify precisely what valuable confidential information you have.

While that may seem obvious, it is the most critical, but often missed, part of the plan. Many trade-secret misappropriation claims have flopped because the first time the complaining company cataloged its trade secrets was after the claimed misappropriation occurred—like closing the proverbial door after the horse is out of the barn.

Once the information is cataloged, step two is securing the confidential information against unnecessary or improper access. Trade secrets are entitled to protection only if reasonable steps are taken to keep them confidential. You should not allow outsiders access to your confidential company information unless they have signed a written nondisclosure agreement. Even within your organization, access to highly confidential information should be strictly limited to those with a genuine "need to know."

Step three is educating your employees. Company policies should be explained on, or even before, an employee's first day of work; delivering that lecture for the first time on the day of the exit interview is not going to get you very far. Employees need to understand from the start that they

