

BALANCING SECURITY AND TRUST

By Carol Hymowitz

Wall Street Journal

August 16, 2005

In today's knowledge-based economy, businesses walk a fine line between being security savvy about protecting their sensitive data, and creating such a Big Brother atmosphere that they trigger the very brain drain they want to prevent.

Technology gives job-hopping employees an easy way to take reams of data with them when they walk out the door. But that same technology also lets companies track exactly what is downloaded from networks. "To create a fair, efficient and innovative work environment, you can't lock everything down," says Michael Allison, chief executive officer of ICG, a Princeton, N.J., corporate-investigations firm.

Businesses often don't decide on a balanced security policy until they're hit with intellectual-property theft. When that occurs, there is not only concern about loss of valuable information to rivals but a feeling of betrayal among former colleagues who once trusted the perpetrators.

The recent lawsuit brought by Korn/Ferry International puts the issues in clear focus. Earlier this month, Korn/Ferry, the world's largest executive-recruitment firm, sued a former top executive and four other ex-staffers, claiming they illegally took valuable candidate and client records. (Related article2)

Michael Kelly, an attorney who specializes in intellectual-property law at Squire Sanders & Dempsey's San Francisco office, suggests that companies take precautions to protect their property, and learn to be aware of early warning signs and the points of contention that often spark a data theft.

"If you've just given someone a bad review, or an employee demands a bonus and you say no, or someone's key customer just canceled business, you should be on the alert," he says.

Employers should also be ready to deal with not only discoveries concerning the alleged offense, but any of a number of issues that may arise when rifling through an employee's files. "You can start out looking for theft and discover the employee is having a romance with the company president," Mr. Kelly says.

He knows of an instance where the company completely lost focus on the theft it was investigating after uncovering a series of messages from one employee lambasting his boss.

More problematic, he says, was the case of one company he represented that checked the email of an employee it suspected was downloading company data and instead found that he was involved in child pornography. It was reported to authorities and the employee was dismissed.

Employees often mistakenly believe their email and computer hard-drive files are their personal property. Companies should explicitly warn their staffs that their bosses have a right to look at their computer files and emails.

On the other hand, they can't stop an employee from remembering the clients and customers they worked with.

"What's in the company computer is company property and taking that is a clear no-no," says Mr. Kelly. "But things are a lot grayer if, after you leave an employer, you write down the name of every person you can remember ever having done business with, and then try to reconstruct your old files."

It used to be that a departing employee had to pore over phone books to collect mailing addresses and telephone numbers of contacts; now, the Internet can facilitate reconstituting a contact list.

There's also nothing wrong if an employee uses the general knowledge he or she gained at a prior employer, such as quality-control practices or successful business strategies. It's a different story if an employee memorizes, and then duplicates, the secret formula of a company's brand-name soft drink, for example.

So, what happens if a talented or valued employee who has worked on a critical product or been privy to sensitive company strategy jumps ship to a rival?

Microsoft and Google currently are locked in a legal fight over a highly regarded former Microsoft executive, Kai-Fu Lee, who in July moved to Google as president of its China operations.

Microsoft alleged in a suit it filed in Washington state, where it is based, that Dr. Lee violated his employment contract when he took the Google post, and earlier this month won a restraining order preventing him from beginning his new job.

In its suit, Microsoft said that "as a condition of becoming an executive at Microsoft, Lee agreed to ... a limited noncompete agreement, aimed at protecting Microsoft's confidential, proprietary and trade-secret information." Noncompete agreements generally state that an employee won't work for a rival firm doing the same work or work using the same skills for a certain time after they depart, usually one year.

California-based Google fought back by filing a suit in that state -- the only state that doesn't permit noncompete employment contracts -- accusing Microsoft of using scare tactics to stop Google from hiring its employees. Google says Dr. Lee isn't divulging to the company what he learned at Microsoft.

"Google hired Dr. Lee for his strong management ability and leadership skills," said Nicole Wong, associate general counsel at Google.

Central to the case is whether Dr. Lee's job at Google will compete directly with work he performed at Microsoft. In its suit, Microsoft alleges that Dr. Lee for a time was responsible for Internet search and was a key architect of its Beijing research lab, among other things. But in a sworn statement, Dr. Lee alleged that Microsoft CEO Steve Ballmer told him before he quit, "It's not you we are after, it is Google."

Both companies are battling for dominance in Web-search services, with Google, which has hired a number of Microsoft engineers this year, in the lead.

Rather than costly litigation, companies often choose to negotiate with a rival company that has snared a valued employee to make sure he or she doesn't divulge proprietary information or work in a competitive area. But companies must distinguish between their right to protect intellectual property and their use of restrictive employment contracts, says Cliff Palefsky, an employment attorney at McGuinn Hillsman Palefsky in San Francisco.

"If a company has a right to fire you when they want to, how can they say you can't take a job with a competitor?" he asks. "Telling an employee he can't do that when you're no longer paying him is a form of indentured servitude."

The best defense against talent loss and intellectual property seepage, of course, is good management. Companies in certain specialized fields will be competing for the same small pool of talent.

"If you don't force them to sign a noncompete, they may be more likely to work for you than the company that requires one," says Mr. Kelly.

And if you respect them and pay them well, they're a lot less likely to job hop, or if they do, to turn around and use the knowledge they gained to do you harm.