Zipping Lips

By Elizabeth Freudenthal, California Law Business Journal

Technology and a fluid job market have increased the chances for rogue employees and contractors to leak confidential information. In response, companies are putting tighter restrictions on workers.

Late at night, long after pizza joints and video rental stores had closed, an employee of a financial consulting firm logged onto the Internet under a fictitious name and published secret details about the merger plans of a large tech company in the Bay Area.

The company, which had hired the consultants to help in merger negotiations, had obtained confidentiality agreements before providing access to the company network and to executive communications.

Imagine the company executives' reaction after reading about its closed-door discussions on the Web. Not surprisingly, the victimized company filed a John Doe complaint in a Bay Area superior court, which allowed it to trace, through a subpoenaed Internet service provider, the leak back to its own merger consultants.

Corporate betrayals like this one are why companies are increasingly concerned about protecting their proprietary information.

Today's companies depend more on consultants, temporary workers and vendors. Along with increased use of outsourcing, corporate partnerships and affiliations have become more common. Such alliances often require exposing proprietary information to outsiders: the specialist setting up an intranet, the contract programmers designing a company's Web site and the financial consultants analyzing a company's prospects in e-commerce all have more ways to access trade secrets and more opportunities to do so.

"As we invent new technologies and trade secret protection becomes more important to protect them, we are also creating tools that make [trade secrets] more vulnerable," say James Pooley, an intellectual property litigation partner at Gray Cary Ware & Freidenrich in Palo Alto.

Along with technological advances, the business practices of high-tech companies have contributed to the trade secrets crisis. New companies are often spun off from -- and compete with -- the parent companies. And some industry insiders complain that the high-tech market moves too fast for patents to be relevant.

As a result, many California companies are bolstering their IP-protection policies, not only for their own employees, but also for the increasing number of non-employees who have access to sensitive information. Their strategies range from minor, but important, changes to standard confidentiality agreements to much more elaborate and expensive measures.

Oakland-based Clorox is one of the companies that uses detailed, individualized confidentiality agreements to compensate for any gray area inherent in existing regulations. "We don't rely on statutory or common law doctrines, "says Joel Hayashida, corporate patent counsel at Oakland-based Clorox Co. and past chair of American Corporate Counsel Association's national intellectual property committee.

Hayashida refers primarily to the work-made-for-hire provisions in the Copyright Act of 1976. The law specifies that a company owns certain kinds of work created by its employees or contractors, but the categories of work allowed under the doctrine do not cover such areas as software design. Moreover, even when work fits in a given category, the employer and employee must sign a contract that states the employee was specifically hired for making copyrightable works for the business.

"We try to have the consultants agree to assign copyrightable subject matter to us, beyond the work-for-hire-doctrine," says Hayashida, who adds that contracts not only clarify ownership of future ideas, but also require non-employees to protect a company's existing proprietary information.

In addition, Clorox follows a checklist of security procedures including issuing security badges with digitized photos, logging all telecommunications and monitoring expense reports and time sheets.

Clorox also requires employees and contractors to undergo entrance and exit interviews. Upon entrance, trade secret liability is specifically discussed. Upon exit, the departing worker hands over physical security items like keys and passes. In addition, the worker reviews and provides written documentation of all the work he or she was hired to produce.

Other companies have followed Clorox's example and see no need for further protection beyond creating specific, individualized consultant contracts and enacting basic security measures. For example, Midland, Michigan-based Dow Chemical relies only on contracts to protect trade secrets, despite its recent spate of litigation that include a lawsuit filed in July against two former employees who later became technical consultants.

Sharon Orieo, director of intellectual asset management at Dow's technology center, says that the recent suit is an example of the company's strict enforcement of current policies, but that "it has not caused any major changes."

"We have secrecy agreements in place with [consultants,] each crafted for that particular situation," says Orieo. Each consultant signs an agreement individualized according to the job at hand as well as the length of time the relationship will last. Contracts do not include specifics about what parts of the campus or the computer network consultants can access. Instead, the job dictates access; consultants brought on to refine a certain chemical formula will see no other formula, and no non-employee has wholesale access to physical facilities or computer systems. Nonetheless, there are a few companies that consider nondisclosure agreements, even customized ones, useless when trying to protect information.

Perhaps one of the more extreme examples is Synopsys Inc., a Mountain View-based company whose products automate parts of the manufacturing process for electronics systems. About five years ago Sylvia Nessan, Synopsys' director of worldwide corporate and community programs, worked with **Naomi Fine, founder of San Leandro IP protection consulting firm Pro-Tec Data**, to develop what they call "SURF"-secure user research facility. SURF is a separate building on each of the four major Synopsys campuses, for Synopsys' business partners and customers to use while working with the company.

With no physical or electronic links to the Synopsys system, each SURF building has its own entrance and exit, secure phone and network lines, reinforced ceilings and security system as well as its own employee amenities like kitchens, break rooms and conference rooms. Synopsys employees cannot enter SURF without authorization by the guest company.

Nessan says she developed the SURF concept to protect Synopsys' own trade secrets, and to attract more business by protecting its clients and partners' trade secrets. While few companies can afford to take such expensive measures as building a separate facility when simply hiring a few temporary programmers or financial analysts, there are plenty of additional protective measures companies can enact.

Following Clorox and Dow's lead, Pro-Tec's **Fine recommends, for example, a few simple additions to the standard secrecy contract.**

"Include many of the specific details that are likely to be found in the employee policy but are too specific for nondisclosure agreements," she says. "Specify very clearly what the non-employee is supposed to do with respect to information."

For example, employees may be told, via an employee handbook, precisely which types of documents need to be shredded, which need to be labeled as confidential or which need to be filed in certain places. Temporary employees, who don't see an employee policy handbook, ought to see those rules in their contracts.

In addition, Fine suggests including in the contract a "triggering event." Examples include making payment contingent upon an exit interview to ensure that the specified protective measures are actually followed. And when hiring workers from a temp agency, many companies are asking individual temporary workers to sign a contract instead of giving one sweeping agreement to the temp agency director.

But Fine admits that these solutions are "very cumbersome and logistically difficult." So with the participation of several of her clients--including Safeway, Seagate Technology Inc. and Varian Associates Inc.--she is developing an Internet application that she claims will improve current methods of protecting a company's trade secrets when working with non-employees. Fine declined to describe the product further.

In the meantime, experts suggest alternative precautions. Gray Cary's Pooley says a growing number of companies have a basic "checklist approach" similar to what Clorox's Hayashida describes.

Common elements of the checklist include visitor-access control, such as examining briefcases and making each visitor sign a blank sheet of paper, so visitors cannot see names of others. Companies are tightening up computer-system security by using passwords, secure connections and message encryption.

The most cost effective method, however, is educating management about the policies and procedures, Pooley says. Managers are then able to oversee that all precautions are followed.

Tom Seaney, manager of information protection at Palo Alto's Sun Microsystems, agrees that trade secret protection can be accomplished by simple means.

A primary precaution Sun takes is a "Sunscreen," a background check given to any worker with access to Sun's network and physical facilities, including temporary workers, consultants and permanent employees. The check does more than prevent Sun from hiring people with a history of trade secret theft. The check also increases a culture of trust among Sun's employees, which, according to Seaney, does more to prevent trade secret theft than any statute could.

Like other corporate security managers, Seaney and Clorox's Hayashida believe that non-employees should follow the same rules employees follow. But given the unique fluidity of Silicon Valley's workforce, the opposite is also true, attorneys say. High-tech employees change jobs so often that for the purposes of trade secret protection, they might as well be treated as temporary employees.

"We're seeing a bit of a sea change in the way we're looking at employee departures," says Gary Weiss, co-managing partner of Orrick Herrington &

Sutcliffe's Menlo Park office who specializes in trade secret theft, employee raiding and unfair competition. "People are flitting from job to job with increasing regularity and speed, so that issues that come up with respect to temporary workers in effect come up with regular workers."

Weiss recommends specifically reminding new hires and new non-employees, during entrance interviews, of their obligations to their old nondisclosure contracts. Then if the company is involved in future litigation, it can say it has made efforts to protect its secrets as well as other companies'.

But Fine and others caution that treating non-employees exactly as employees may raise serious employment law issues. **"While recognizing that a lot of these people are sitting side by side with their employees, accessing equal or greater amount of information, companies have to be very cautious not to provide the same amount of resources to employees as to non-employees,"** Fine says. If employers transfer employee status to non-employees, they are liable for a whole different set of legal complaints.

Because of such complexity in trade secret protection, many attorneys agree that companies have increased their awareness of the topic. "Employers have become more vigilant right at the beginning," says Orrick Herrington's Weiss. "As an employer, you need to do more than look the other way and assume everyone's going to do the right thing."

This article was originally published in the California Law Business Journal, October 1999. © Daily Journal. Reprinted with permission.