Avoiding Danger to Business Secrets in a Bad Economy

David Walton
Special to Law.com
January 9, 2009

Bad economic times create opportunities for strong companies to poach good employees from a weakened competitor -- a signal for employers to aggressively protect trade secrets.

In fact, employees in sour economic conditions are apt to switch companies to head off potential job loss. This is especially true for workers controlling or having access to a "book" of business. For these employees, their book is their life. Oftentimes, their compensation at the new company is contingent, in part, on how much business follows them.

These employees can be desperate to keep their clients, sometimes believing they belong to them -- not the company. If the employee is subject to a non-compete or a non-solicitation agreement, the company may have adequate protection. But, where there is no non-compete, or the employer plans to circumvent it, companies are at high-risk for having their trade secrets and confidential information depart with key employees.

Here's a look at steps companies and their counsel can take to prevent trade secret theft and to act effectively if they believe a departing or new employee has stolen critical information.

SPOTTING A COMPANY SPY

I'm often asked if there are any key indicators an employee is getting ready to leave. In hindsight, it's easy to say, "I should have known a former employee was up to no good when 'X' happened." But, frequently, employees who take trade secrets and confidential information are trusted, long-term employees. Even so, there are some things an employer can watch out for when a key employee is secretly preparing to go to a competitor, including:

**Unusual requests for client meetings.** Employees secretly planning to leave often ask for permission to meet with clients to discuss a special project or initiative. If the employee normally does not meet with customers or is not required to, then think twice before giving the green light.

**Late night e-mail/system access.** Employees who steal confidential information often do it right before they leave. Look out for anything unusual -- i.e., late night/weekend access to sensitive databases, electronic information and key-card building access -- as a potential sign that the employee might be up to something.

**Unusual requests for confidential information.** After an employee has decided to join a competitor, he/she may request access to highly confidential and sensitive material that's not normally accessed. The plan, of course, is to surreptitiously copy or even memorize this information.

DEFENDING TRADE SECRETS

Red flags or not, there are important steps an employer can take right now to prevent breaches, and help establish that its information is legally confidential and deserving of trade-secret protection:

**Limit access to highly sensitive material.** If all your employees have access to something, then is it truly
confidential or deserving of special protection? Most courts say "no," so be careful to whom you give access when dealing with your most important information.

**Set up computer systems to prevent flash drive use.** Flash drives are the number one way to steal trade secrets. Don't let your employees use them, if feasible. If not, ensure they use only company-issued flash drives so you can demand their return upon termination.

**Use confidentiality agreements and restrictive covenants.** If enforceable in your particular jurisdiction, using restrictive covenants (i.e., non-compete and non-solicitation agreements) is the best way to protect your trade secrets and confidential information. Confidentiality agreements are also useful, because they show the judge and jury that: (1) the employee had notice that specific information was deemed confidential; and (2) the employer took reasonable measures to protect its information.

**Use exit interviews.** If an employee resigns, immediately cut off access to email and computer systems. Conduct a comprehensive exit interview with the employee as soon as possible. During this meeting, remind the employee of any post-employment covenants, and ask directly if he/she is taking any company information or has already stored it on a home/personal computer. Demand that all of this information be returned, as well as BlackBerrys and other employer-owned devices. In addition, have the employee sign an acknowledgment that all information was returned and that he/she is not permitted to take any trade secrets or confidential information.

**COMBATING A VIOLATION**

What do you do when an employee leaves and you suspect foul play?

**Resist self-help.** Many times, after an employee leaves under suspicious circumstances, the IT Department cracks open the former employee's computer and searches tons of email. But, in doing so, many internal IT employees do not use forensically-sound methods that avoid the tainting or even mistaken deletion of important data. Seek a third-party forensic expert, who is more objective and not subject to strong bias arguments in court.

**Freeze all media.** Once the employee leaves for the competition, freeze and preserve his/her computer and all other employer-issued electronic media like cell phones, PDAs, flash drives and portable hard-drives. If the media is turned on, leave it on. If it's turned off, leave it off. A simple booting or shutting down of a computer can permanently delete important information. If you need to put the media back in use, take an image of the hard drive, using forensically sound methods -- and store it in a safe place in case it later needs to be searched. Many great cases have been lost because these steps were not followed.

**Save the email.** If you work with a Microsoft exchange server for your email, all users have a custodial space on the server where Microsoft outlook files are stored. This includes all stored and unread email, calendars, email folders and contacts. If an employee leaves and you suspect foul play, get a copy of this custodial "box" for the employee and secure it. Many times, emails are the best way of proving nefarious activity.

**AVOIDING A LAWSUIT**

So, what do you do when you're the employer doing the hiring? How can you ensure you are not hiring a lawsuit? Here are some keys:

**Disclose all post-employment obligations.** Before hiring any employees from the competition, ask for all restrictive covenants. If the employee tells you he/she doesn't have any, get it in writing.

**Acknowledge compliance.** Ask the prospective employee to sign an acknowledgment promising: (1) to comply
with all post-employment restrictive covenants; and (2) not to disclose any of the former employer's trade secrets or confidential information.

**Don't take anything.** Caution the prospective employee about taking or retaining information belonging to his/her former employer. Confirm that the employee doesn't bring any of this information. And, if he/she has information, it must be disclosed or returned to the former employer before joining your company.

**Don't tell or recruit.** The line between legally proper behavior and improper conduct breaching the duty of loyalty is a very murky one. To be safe, the prospective employee shouldn't tell any colleagues about departing the company before officially resigning. And, he/she must not recruit or solicit any employees to leave.

**Don't wait.** Dare to hire an employee from the competition? Move fast. The longer the employee stays after accepting your final offer, the worse it looks. Juries rarely believe that an employee who receives an offer several months before resigning was sitting around actually mulling the offer. In this scenario, a jury may infer the employee was poisoning the well or setting-up a mass departure -- even if the worker had good reasons for waiting to resign. So, once a decision is made to switch companies, be sure your future employee resigns quickly.

Hiring employees from the competition is fraught with great business upside, mixed with legal peril. Whether you're the company losing the employee or the new employer, following these steps will greatly improve your legal position and ultimately minimize the threat to your business.

*Cozen O'Connor labor & employment attorney David Walton represents a broad range of clients, from large multinational corporations, to small companies -- litigating matters involving non-competes, restrictive covenants, trade secrets, fiduciary duties and discrimination claims, and assisting employers facing challenges posed by the information-age economy. Vice-chair of the firm's E-Discovery Task Force, Walton recently won a $7 million jury verdict on behalf of a U.S. company whose trade secrets were stolen by former employees. Contact him at dwalton@cozen.com or 610-832-7455.*