Safeguarding Trade Secrets Before, During and After a Reduction in Force

By Allegra Lawrence-Hardy and Jim Johnson

In these difficult financial times, reductions in force are increasingly common. If an employee must be ushered out the door, take care not to usher out the company's trade secrets at the same time.

Trade secrets, especially those stored electronically, are typically portable. For this reason, terminated employees can easily walk away with trade secrets whether intentionally or inadvertently.

To safeguard trade secrets, employers should keep the following tips in mind before, during and after reductions in force. Even if the company is not contemplating a reduction in force, these tips are useful any time an employee departs.

First, what exactly is a trade secret?

A strong technology policy coupled with an equally strong trade secrets policy prompt employees to think twice before spilling secrets online.

Trade secrets, which are protected by state law, include information such as a company's financial and pricing data, or customer lists. Most states, though not all, follow the Uniform Trade Secrets Act, which defines a trade secret as information that "(a) derives independent economic value (actual or potential) from not being generally known to, and not being readily ascertainable by proper means by, other persons … and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

Under the Trade Secrets Act, if a company, upon losing a trade secret, wants to establish a legal claim for misappropriation, the company must be able to prove it has taken reasonable steps to preserve the secrecy of that information.

Of course, preserving secrecy is more important for business purposes than for potential litigation purposes. Although it is prudent to think ahead to potential misappropriation claims, the real goal is to keep the information out of the hands of competitors now. To that end, the following tips can help employers safeguard trade secrets before, during and after a reduction in force.

Before a Reduction in Force

Well before announcing an impending reduction in force, an employer should include in the employee handbook comprehensive trade secrets and technology policies. Trade secrets policies should explain, for example, what trade secrets are, why they must be protected and what disciplinary action will result if they are compromised.

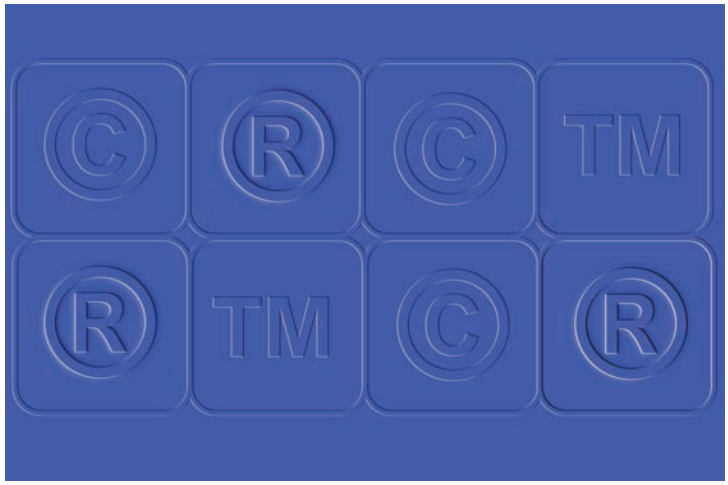
As employees are let go, steps should be taken to ensure that they cannot upload data to Web sites that allow one to transfer large amounts of information easily via e-mail.

Employees should be required to sign an acknowledgement form, indicating their understanding and agreement with the company's trade secrets policy.

Technology policies should inform employees that their use of electronic devices is subject to monitoring. For example, an employer should make clear that nothing on a work computer is private, even personal Web mail. A strong technology policy coupled with an equally strong trade secrets policy prompts employees to think twice before spilling secrets online.

Implementing a technology policy requires a company to make choices about how to keep tabs on employee computer use. Methods range from monitoring live use in real time, to taking timed screenshots, to automatically recording a log of a user's activity.

Additionally, "sniffers" enable information technology specialists to capture packets of electronic information sent to and from a user's computer, thereby allowing the company to reconstruct any online activity that has occurred.



Obviously, employees will consider some methods more intrusive than others. This perception and its effect on employee morale might be a factor in deciding which method is right for the company's culture.

Regardless of which methods the company chooses, there are two things to keep in mind when monitoring employee computer use.

First, be sure to install the monitoring software on all employee computers, not just those used by certain employees. Even if the company does not think it necessary to monitor all employees, installing the software across the board promotes fairness and objectivity.

Second, be prepared to react if an employee engages in inappropriate activity. If the employee is divulging trade secrets, follow through with disciplinary action as outlined in the employee handbook.

If he or she is engaging in some other inappropriate activity, such as harassing another employee, be aware that the company may have to get involved.

For example, the New Jersey Supreme Court has held that an employer had a duty to stop harassment on an electronic company bulletin board when it became aware of such activity, and courts elsewhere may do the same. *See Blakey v. Cont'l Airlines*, 164 N.J. 38 (2000). Again, be prepared to react to any inappropriate activity discovered.

During a Reduction in Force

To make a reduction in force as smooth as possible and avoid potential problems, follow clear exit procedures.

As far as trade secrets and technology are concerned, the company's exit procedures should ensure that each employee returns all company property, including laptop computers and all electronic storage media.

Designate which department is responsible for collecting electronic devices, whether it be information technology, human resources or some other entity. Those who collect the devices should understand their role in protecting the company's trade secrets. They will have the first opportunity, for example, to notice a missing Blackberry that may contain a contact list that potentially could be a trade secret.

As employees are let go, steps should be taken to ensure that they cannot upload data to Web sites that allow one to transfer large amounts of information easily via e-mail. Employees' access to work computers should be blocked.

In addition, their hard drives should be imaged and maintained for a prescribed amount of time. Perhaps most importantly, if there is reason to believe a problem might arise, the particular employee's electronic devices should be closely scrutinized as discussed below.

After a Reduction in Force

Once employees have returned their electronic devices, the company's IT department should identify any red flags, such as a hard drive that has been wiped clean.

If any red flags are discovered, the IT team should refrain from further investigation because, in the event of litigation, evidence will need to be preserved. At this point, the company should consider whether the situation warrants the services of a forensic examiner.

Such services are often quite expensive and typically are reserved for the most serious situations. If the immediate attention of a forensic examiner is not warranted, it still might be wise to store the hard drive or other device in a locked cabinet in case an issue arises later.

Generally, circumstances will not call for forensic examinations or the long-term storage of devices, but only for the maintenance of employees' e-mail, instant messages, voicemail and other electronic files for a prescribed amount of time, such as 30 to 90 days.

These electronic records should be maintained not just for purposes of identifying trade secret breaches but also to ensure the information is available to continuing employees who are taking over assignments or clients when current employees leave.

A company should coordinate its electronic records retention policy with its policy for retaining paper records and ensure that retention policies are formulated with protecting trade secrets in mind.

A reduction in force is seldom a simple undertaking. Do not complicate matters further by allowing trade secrets to follow departing employees out the door.

A reduction in force is seldom a simple undertaking. Do not complicate matters further by allowing trade secrets to follow departing employees out the door. Keeping these tips in mind can help the company keep valuable trade secrets safely in house.

Allegra Lawrence-Hardy is Co-Chair of Sutherland's Complex Business Litigation Practice Group. She has extensive experience handling complex multi-party, class action, multi-jurisdictional commercial and labor and employment matters. She has successfully defended primarily Fortune 100 companies throughout the United States and abroad in numerous trials, arbitrations and other forms of alternative dispute resolution. Jim Johnson serves as intellectual property counsel in Sutherland's Intellectual Property Practice Group where he manages the international enforcement of the trademarks and copyrights of some of the world's most famous and valuable brands. Prior to joining Sutherland, Jim gained extensive trademark experience as in-house counsel for The Coca-Cola Company and Kellogg Company and as an examining attorney at the U.S. Patent and Trademark Office. Thanks to Jessica Sawyer Wang and Carlos Santana for their contributions to this article.