Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# 5 Tips For Employers To Protect Their Trade Secrets

By **Scott Flaherty**

*Law360, New York (February 26, 2013, 7:12 PM ET)* -- With last week's unveiling of a White House-led strategy for keeping America's business trade secrets from falling into the wrong hands, attorneys say the time is ripe for employers to review their own measures for protecting valuable company information.

As companies look at their efforts while remaining attentive to possible legal pitfalls, there are a number of strategies to keep in mind, such as identifying the business's most important information and building trade secret protection into the company's employment policies and technology systems.

"It all goes back to the bottom line of trade secret law: That is, has the company taken reasonable measures to protect the secrecy?" said Kenneth Carlson of Constangy Brooks & Smith LLP. "Companies have to be proactive with trade secret protection. They have to be thinking ahead, because oftentimes, it's not a problem until it's a problem."

Here are five tips for employers hoping to keep company trade secrets from slipping out the door.

## Classify Company Info

Before developing a plan to protect trade secrets, attorneys say, there's an invaluable first step: knowing what company information is most critical and identifying what is already being done to keep the information protected.

A good starting place on that front, according to Seyfarth Shaw LLP's Robert Milligan, is to conduct a thorough review of company information and classify it by level of importance, from "bet-the-company" data on down.

From there, companies can take a closer look at what protection strategies they have already adopted, and locate any potential holes. Those reviews should be done in a "business-specific" fashion, while keeping in mind what type of information a company most wants to keep safe, said Carla Oakley of Morgan Lewis & Bockius LLP.

"Implement security measures that are appropriate for the kind of information that is being protected," Oakley said.

## Keep Employees in the Loop

The legal pitfalls an employer might encounter while trying to protect trade secrets, including those arising under privacy and employment laws, can often be avoided by adopting clear policies upfront and educating employees about the rules, several attorneys said.

"You make it clear to people ahead of time; that's how you have to go about thinking of this problem as an employer," said Richard Shea of Covington & Burling LLP.

One concrete measure is to create a comprehensive employee handbook, according to Matthew Prewitt of Schiff Hardin LLP. If things are made clear early, employers can incorporate policies in the handbook that allow them to, for example, monitor emails or track computer usage, while at the same time staying on the safe side of the law, he explained.

"It's not always cut-and-dry that you can do that unless you have a clear handbook policy," Prewitt said.

Employee handbooks also serve as a good place to spell out a company's policies on social media, a growing concern in the age of Twitter and Facebook. Those policies should include a clear indication that the company has ownership over any work-related accounts, Oakley said.

Beyond a clear handbook, companies should also provide training, on a regular basis, to teach and remind employees of the rules, attorneys say.

"Employee training and education is a key," Milligan said. "If you have employees that get it and understand why it's important ... you're already two steps ahead."

## Check on Incoming and Outgoing Employees

Protecting trade secrets should be kept in mind throughout many of a company's dealings with its employees, starting at the earliest stage of taking on a new hire, according to Stephen Fox of Fish & Richardson PC.

"One thing that goes completely ignored by most employers is the process of thoroughly vetting ... employees," he said.

Once new hires come on board, requiring them to sign restrictive covenants, such as nondisclosure or noncompete agreements, is one way of shoring up a company's legal standing if trade secret information is lost or stolen. But with such agreements, especially noncompete provisions, it's often necessary to pay close attention to the applicable local employment law, which varies significantly by state, according to Michael Elkon of Fisher & Phillips LLP.

Just as it's important to screen new hires, it also makes sense to keep a critical eye on employees who are leaving, several attorneys said. Exit interviews are one standard way to figure out if outgoing employees are headed to competing companies and what their new jobs might entail, and can serve as a way to re-establish any confidentiality provisions they committed to.

Those interviews also present the opportunity to assess an employee's mindset as he or she prepares to depart, something that may key a company in as to whether that employee poses a threat from a trade secret standpoint, according to Prewitt.

"What a lot of companies really fall down on is that they forget [that] people ... and their loyalties change over time," he said.

## Stick to a 'Need-To-Know' System

Restricting the ability of certain employees to access company trade secrets is another way to limit exposure to possible theft of trade secrets from within, attorneys say.

There is often no need, for instance, for all employees to be able to view a company's research and development data or strategic business plans, according to several employment attorneys, who recommended that only employees with an absolute need to see such vital information should be able to do so.

"You want to identify people who have access to information that don't need to have access, and you want to close those walls off," Prewitt said.

In practice, companies can limit access to certain information in a variety of ways, running the gamut from old-fashioned methods, such as locking up filing cabinets and marking confidential documents, to more technologically advanced techniques like creating password-only access to databases and encrypting sensitive information or data transfers, attorneys said.

## Watch Out for External Devices

Monitoring employees' activity on electronic devices goes hand-in-hand with limiting access to critical information, according to attorneys, who said companies should make sure that information on external hard drives, thumb drives or employees' personal computers is well-protected and can be recovered.

Jason Schwartz of Gibson Dunn & Crutcher LLP said employers should ensure they have control over any information loaded on to external devices and have policies in place if a device is lost or stolen. He added that other steps, such as monitoring sizable downloads or emails with large attachments, can help companies quickly detect potential thefts of trade secrets.

The risks posed by external devices have only heightened as more employees work remotely. With those employees in mind, it's important that a company use software programs that allow for a secure connection to its network, according to Elkon.

Businesses should pay particular attention to these types of concerns when employees — especially those in management or technical positions — leave to take a position at another company, Schwartz said. He recommended audits of key employees' activities before they set off to their new jobs, and taking care that all company property and data has either been returned or destroyed.

"When you're going to be attacked from within, they'll usually steal the information literally on their way out the door," he said.

--Editing by Elizabeth Bowen and Katherine Rautenberg.