Lowndes

Here's What You Need To Know About Protecting Trade Secrets

Stephen Thomas

Jan 15, 2020

By: Steve Thomas

The Fine Print

What do you do when a key employee leaves and you believe he/she has taken your company´s trade secrets to a competitor? Or when a strategic business partner uses your trade secret information to compete against you?

The likelihood of recovering damages, or securing injunctive relief, in these scenarios will depend on the steps that were taken to identify and protect trade secret information prior to the breach. As many businesses have learned, deficiencies in your trade secret protection approach can become glaringly obvious in hindsight, and may even prevent recovery of damages or injunctive relief. This is truly a situation in which an ounce of prevention is worth a pound of cure. Failure to adequately protect trade secret information may also amount to an actionable breach of an officer´s duty to the corporation.

There are two common scenarios in which trade secret information is typically lost.

The first scenario occurs when courting potential strategic partners or customers. In the rush to impress such parties, too much information may be shared too soon, sometimes even before confidentiality agreements are executed. The second scenario occurs when employees are exposed to company trade secrets unnecessarily, or without confidentiality obligations. The key in both scenarios is diligence.

The general rules are simple:

1. Never share trade secret information without enforceable confidentiality obligations.
2. Never share trade secret information unless it is absolutely necessary to do so.

Here are some key points from litigated lessons learned:

- Not all confidentiality agreements will protect your trade secrets.

  Beware of any confidentiality agreement that does not specifically address trade secrets. Trade secret information that is shared under a confidentiality agreement that expires without any following requirement for confidentiality may lose its trade secret status, making it fair game for use by anyone. All confidentiality agreements and Non-Disclosure Agreements should be reviewed by qualified counsel. Unfortunately many of these agreements are executed as a matter of course, without legal review, usually due to time pressure.

- Identify, Protect, Monitor.

  If you have never categorized your company´s intellectual assets into trade secret and non-trade secret buckets, you would be wise to do so soon. Be deliberate about the process of identifying this information. Design steps now to keep such information secret. Key steps often include having employees execute fresh, enforceable confidentiality agreements (even as often as at each annual employee review), compartmentalizing information on password protected, encrypted servers (possibly even using nonnetworked computers for this purpose), and establishing access-controlled work areas in which trade secret processes are used. And what about backup files? Are they maintained in a secure manner? You may want to review those cloud backup services agreements. In some instances, trade secret processes may be divided into multiple sub-processes, with no employee having knowledge of the overall trade secret processes. In other cases the process may be easier to manage - for example, in the case in which the process is implemented in software. In such cases, the focus is on protecting the code and preventing code decompilation, even to the point of implementing critical portions of code in a separate firmware device or hard logic. Each situation is specific, requiring a specific technical approach to protection. This is where technically competent legal counsel can make a tremendous difference in creating an effective, streamlined approach to protecting valuable trade secret information.

Once the plan is in place a monitoring system should be implemented. The results of the monitoring should be reported at the executive level, along with a risk

assessment that identifies any individual or entity that represents a risk. Appropriate mitigation should be implemented. These steps are not particularly expensive or time consuming, and they could make all the difference in recovering damages. There are effective statutory tools such as the federal Defense of Trade Secrets Act (DTSA) and state statutes, but these tools generally require that steps be taken to maintain the confidentiality of trade secret information in the first place.

Still, you may be asking if all this is really necessary, as you don´t see your competitors talking about their trade secrets, or the steps they are taking to protect such assets. And that is precisely the point.