Keeping the Secret in Trade Secret

2000-10-01

Probably the most famous trade secret is the formula for Coca-Cola. While the fizzy combination of ingredients brings a taste that is familiar to billions of people around the world, only a handful know what's in a bottle of Coke and in what proportions. How has something so seemingly mundane and widespread fueled the growth of the world's most successful soft drink empire? By being secret, and by Coca-Cola zealously guarding that secret.

Nearly all companies have trade secrets. They can be as complex as a data model for a software program or as simple as a list of customer contacts. The Uniform Trade Secrets Act, which has been enacted in most states, describes the range of items that may be trade secrets broadly as "information, including but not limited to, a formula, pattern, compilation, program, device, method, technique or process . . . ."

It is the very element of secrecy that is critical to the holder of this valuable information being able to get the legal protection provided by that law, and a federal criminal statute called the Economic Espionage Act (18 U.S.C. § 1839). As the Uniform Trade Secrets Act describes it, information can be a trade secret if it "[d]erives independent economic value, actual or potential, from not being generally known to, and not being readily ascertained by proper means by, other persons who can obtain economic value from its disclosure . . ."

As many companies have painfully learned, maintaining secrecy can be difficult in an era of

easy information transfer, rapid employee turnover and contract consultants. To minimize the possibility that valuable information is lost through carelessness or subterfuge, companies must put into place systematic programs to ensure that their trade secrets remain secret. The steps that serve as real world protections against loss are the same as those that a court will consider in determining whether to provide legal protection to something that a company believes is its proprietary information.

While the specifics of any program will depend on the size and character of a company and no single step is determinative of whether adequate protections are in place, some of the steps that management should consider are the following:

Designate a corporate security officer. A company should designate one person who is charged with developing and implementing security policies. Employees should be informed that any incidents of theft or economic espionage should be reported to this security officer.

Employee Confidentiality Agreements and Certifications. All employees, regardless of position, should sign confidentiality agreements in which they acknowledge that they are legally obligated to protect the secrecy of the company's proprietary information. Depending on the circumstances, a company can consider having periodic certifications by employees of compliance with the confidentiality policies of the company, perhaps in conjunction with employee performance reviews.

Entrance and Exit Interviews. The security officer should conduct entrance and exit interviews with employees in which he or she explains the company's policies on the secrecy of proprietary information to all. In the exit interview, the security officer can explain to a departing employee that he or she may use the skills and general knowledge obtained with the company, but not specific proprietary information. The company also may consider having departing employees sign certifications that they are not taking any proprietary information

with them.

Limit Vendor and Consultant Access. Restrict the access to corporate information of even the most trusted vendors and consultants, even if relationships are well established. Vendors and consultants should sign confidentiality agreements and should be closely supervised. The company should have in place access restrictions such as project-specific passwords that can be altered when a consultant's assignment is completed.

Restrictions Among Employees. Access restrictions also may be appropriate among employees. For example, passwords, encryption or other security can be used to limit certain information to particular individuals or work groups.

Document the development of valuable material. This step helps define with precision what information may be proprietary and, together with other security measures, fosters an understanding among employees that the creative processes and information they develop are critical assets of the company.

Business Plan Precautions. Take special care when disseminating business plans. Anyone outside the core management team, including potential investors and lenders, should be subject to a confidentiality agreement before reviewing information on technology, business strategy and other important matters.

Your company's proprietary information could be the proportions of ingredients in a soft drink, a list of decisionmakers at your key customers or how to solve a particular software design problem. If that information is valuable because others don't know it, taking steps to preserve its secrecy is vital to protecting your legal rights and your company's future.

David Wilson

david.wilson@haledorr.com

Republished with permission from *Potomac High Tech Journal*.