Economic Espionage and Maintaining Trade Secrets

Measures for preserving information, value and ensuring future company viability

Patrick McNamara, Scarinci Hollenbeck*

By now we've become all too familiar with the following scenarios: a laptop containing vital information is lost by a key employee in the public or private sector; or perhaps a disgruntled employee on his or her way out the door walks out with valuable company information, and either pirates it by improperly giving or selling it to a competitor, or displays some of it on the Internet for all the world to see. While government at both the state and federal levels has taken some steps to protect this type of information, much more needs to be done in the way a company conducts its everyday business to protect critical information, preserve its value and, perhaps, the very future of the company itself.

The Economic Espionage Act of 1996 was a major step by the US government to address this issue, both at the domestic and foreign level. In recent years all but four US states have adopted some version of the Uniform Trade Secrets Act in an effort to address the situation, recognizing the need to provide business the ability to protect information that is vital to day to day operations.

With the increased focus on preventing acts of bioterrorism or other forms of attack on the food supply, additional focus has again been placed on the strategies utilized by companies to protect trade secrets. Unlike patents and copyrights, trade secret protection can last indefinitely, so long as the protectable information remains secret. Unique products, drawings, lab notebooks, test data and training manuals, as well as sales and customer information, are only some of the types of information which fall under the panoply of "trade secrets." To protect trade secret information, it is advisable for a company to have a written trade secret protection policy. Such a policy advises all employees how to identify, manage and protect trade secrets. It also provides management with a valuable tool in those situations where, as the result of new joint ventures or other efforts in research and development, certain information that is considered proprietary must be revealed to outsiders. It also demonstrates a company's commitment to trade secret protection, which can be important if litigation ensues over alleged misuse of such information. It is also advisable to schedule periodic presentations to reinforce and update employees on companies' trade secret protection goals and procedures. Employees' involvement in the development and maintenance of the trade secret maintenance system will only strengthen their commitment and vigilance to the system itself.

At its most basic level, disclosure of information considered a trade secret should be limited to employees who require such information to perform their duties for the company. There should also be a uniform system for managing documents containing information that would fall under a trade secret protection policy. Otherwise, without such a system, your company may not be able to prove that a document was improperly disclosed, or that it was disclosed under the terms of a confidentiality agreement. Companies also need to maintain separate and locked depositories in order to make sure that unauthorized employees or other third parties do not have access to proprietary information. The same thing can be accomplished with computer records by using an isolated machine with limited password access for proprietary files; other viable steps range from restricting public access to facilities to making sure that outside parties have entered into confidentiality agreements before such information is made available.

It is also important to develop a policy to manage unsolicited suggestions or inventions or ideas from other third parties. Such procedures usually include developing a written notice sent to any person submitting an unsolicited disclosure notifying them that the company will not enter into a confidential relationship with them. An alternative is to request such person to sign an acknowledgement that the company is not obligated to use the information, owes no duty of confidentiality to that person, and that no contractual relationship has been entered into by the receipt of the unsolicited information.

While there is no one single factor that a court will look to in making a determination as to whether information was maintained as a trade secret, there are certain items that courts have looked to in making a determination that a company was not maintaining this information in a proprietary manner. Such actions have ranged from

*The views expressed herein are the author's own.

> Much more needs to be done in the way a company conducts its everyday business to protect critical information, preserve its value and, perhaps, the very future of the company itself.

the distribution of technical literature or other material that discloses a trade secret; failing to obtain signed and executed non-disclosure agreements or confidentiality agreements; leaving the information in unlocked file cabinets or in unrestricted areas of the company; leaving documents disclosing trade secret information in garbage cans without shredding the documents; identifying a trade secret in any type of government filing, or in a foreign or international patent application that may disclose the trade secret; or in any type of court proceedings where no request is made to seal the record.

In sum, with technology and new forms of electronic communication continuing to challenge the ability of the government or the courts to keep pace, it must become part of the everyday culture of a company to protect and preserve trade secret information. This "culture change" has to become part of the everyday operation of a company, and not something discussed once or twice a year at a meeting in a conference room.

Address correspondence to pmcnamara@scarincihollenbeck.com.