



Jon S. Liland  
Direct dial: 603.643.9070  
Fax: 603.643.3679  
jliland@sheehan.com

### Practice Areas

Business Formation and  
Succession Planning  
Corporate Law and Governance  
Entertainment, Media and  
Publishing  
Mergers and Acquisitions  
Private Companies and  
Professional Practices

## Good Company

### Get With the Program: Protecting Your Trade Secrets With a Trade Secret Protection Program

Wednesday, August 04, 2010

New Hampshire's Uniform Trade Secrets Act (the "NH UTSA") provides strong protections for companies that use certain types of confidential information in their businesses. The statute defines broadly the types of information that qualify as trade secrets, and provides for substantial remedies for a company whose information has been wrongfully disclosed, including injunctive relief, compensatory damages and punitive damages.

However, not all valuable confidential information is automatically protected. Under the statute and existing case law, any business which seeks to protect information as a trade secret under the NH UTSA must make efforts that are "reasonable under the circumstances" to maintain the secrecy of that information. Whether or not the secrecy protections a business has put in place are reasonable is a question of fact to be decided by the court in any litigation, but the party seeking trade secret protection bears the burden of proving that the measures were appropriate under the circumstances. If that cannot be done, then the information will not be protected by the court, regardless of how damaging its disclosure may be.

It is essential, therefore, for any business which has valuable confidential information to adopt a carefully planned and thoughtfully implemented trade secret protection program. Too many businesses, especially emerging businesses, focus entirely on the creation and development of new intellectual property, with scant attention given to the protection of that property after it has been created. The result is that safeguards are implemented in a piecemeal fashion, based upon incomplete, anecdotal evidence as to what others in the marketplace are doing, and without the strong management support necessary to make effective protection of intellectual capital part of the everyday culture of the business.

Having a well organized and clearly documented trade secret protection program serves two vital functions - first of all, it will almost always provide much more effective protection for the trade secrets of the company than safeguards that are developed on an ad-hoc basis, thus reducing the chances that the company will need to incur the costs and risks of litigation to protect its intellectual capital. Secondly, it will allow the business to demonstrate clearly in any litigation that it had comprehensive safeguards in place that were reasonably designed to prevent disclosure of its information. Even though in a particular instance those safeguards may not have been effective, the court should protect the information against disclosure pursuant to the NH UTSA. In addition, a well-designed and consistently administered plan will demonstrate to the court and to the wider world the seriousness with which the company approaches the

protection of its information, and thus the value that the company places on the information and the likelihood that it will take action to protect that information from disclosure.

Because every enterprise faces different threats to the confidentiality of its trade secrets, there is no "one size fits all" approach to the development of a trade secret protection program. An effective and enforceable program must be carefully tailored to the business in question and the risks it faces, and should ideally be developed with the cooperation of appropriate counsel. That being said, there are some basic, general principles which apply to all businesses.

One key aspect of any program is communicating effectively with employees, contractors and visitors to the company's facilities, so that anyone who may come in contact with the confidential information is aware both of the importance of keeping the information confidential and that the company will take steps to protect that information from disclosure. After all, it is not reasonable to expect someone to comply with restrictions they were not aware of, with regard to information they may not have known was confidential.

With regard to employees in particular, this will entail having clear guidelines for what information is considered confidential, how that information is to be used, and who has the right to access it. Although it is important to have provisions on this point in an employee manual or other policy compilation available to employees on an ongoing basis, the more effective way to communicate this to individual employees is as part of the hiring process. Depending on the circumstances, this communication can be as informal as an oral communication made as part of every new employee's orientation, or can be documented as part of an employment agreement or separate confidentiality agreement executed by the employee. Any oral communications should be formalized and documented (using standard notes for the presentation and a hiring process checklist to confirm attendance of the employee, for example).

Restrictions documented in an agreement with the employee can be as simple as an acknowledgment by the employee that he or she will have access to confidential information, that such information is valuable to the company, and, as a condition of employment, the employee commits to preserve the confidentiality of that information both during employment and thereafter. In a situation with more sensitive information, or particularly where that information may have significant value to any subsequent employer of the employee, the company may want to consider a more comprehensive agreement specifically restricting the employee's ability to compete with the company after termination, for a reasonable period of time; in addition, the company may want a commitment from the employee that the employee will notify future employers of such restrictions, and notify the company of the departing employee's new employer and nature of the job when the employee leaves.

Other parties who will need to be notified of, and bound by, confidentiality restrictions include visitors to company facilities, potential transactional counterparties (including potential financing sources or acquirers), and potential licensees of the company's technology.

If visitors to the company's facilities, such as equipment service people, union officials, government officials (such as building or fire inspectors), and customers could be exposed to confidential information on their visit, then the company should institute appropriate precautions. The extent of the restrictions that are reasonable will depend on how easily the confidential information could be revealed from a site visit, and the nature of the site itself; a balance has to be struck between effective protection on the one hand, and practical efficiency on the other. At a minimum, any visitor to a sensitive site should be required to check in with a log book communicating basic confidentiality restrictions upon arrival. In a large company, where visitors are difficult to distinguish from employees, each visitor should be provided with a badge identifying them as a visitor, and employees should be instructed to approach any unescorted visitor on the premises to help them in finding the person they seek. In some circumstances, it could be appropriate to require every visitor to have an appointment, so that company staff can be prepared for the visit, or to verify through a telephone call the credentials of every visitor, so that unauthorized persons cannot gain access by claiming to be someone they are not, such as a telephone or utility employee, police officer, or the like.

Potential investors and potential transaction counterparties who will have access to written confidential information (whether maintained in a tangible writing or electronically) should always be required to enter into a comprehensive confidentiality and non-disclosure agreement identifying the nature of the confidential information, the restrictions on the use thereof by such person, and the consequences of any violations. The agreement should be very clear that the company has the right to enjoin any violation, or threatened violation, of the restrictions in the agreement, and to seek appropriate damages. For highly confidential information, the best practice is to mark each and every document containing such information with an appropriate legend, either on the cover thereof or even on each page thereof.

As is probably clear from the preceding discussion, the substantive restrictions to be communicated will depend on the nature of the business and the trade secrets that are being protected, and will need to be developed by someone with extensive knowledge of the company, the information being protected, and the company's relationships with its employees, visitors and other third parties. One important consideration is the extent to which access to the information is restricted to those employees or others who have a legitimate need to know the information. In the leading New Hampshire case decided under the NH UTSA, *Mortgage Specialists v. Davey*, the New Hampshire Supreme Court rejected a mortgage company's attempt to protect its information, including customer contact information, from disclosure by two prior independent contractors in part because the allegedly confidential information was stored in an attic at the company's offices that was readily accessible to all employees and contractors, and was not marked "confidential" or "trade secret." Examples of ways of restricting access under appropriate circumstances include password protection for electronic documents, locked cabinets or storage areas for tangible documents, and restrictions on printing or copying of particularly sensitive materials.

Other restrictions will need to be developed by each company in light of its activities. As one example, a chemical company may develop innovative manufacturing methods through the efforts of its employee chemists, who may also have an interest in contributing to scientific journals or symposia as part of their professional development. It may also have workers on the line who understand their particular jobs quite well, but have little insight into the actual chemical processes involved in making a given product or any of the confidential information of the business. A company in this situation would need to have a policy requiring that any writings published by a chemist be reviewed and cleared by an appropriate company representative in advance of any publication, but would have little concern about publications by the line employees.

Designing and adopting an appropriate trade secret protection program requires that management invest significant time and effort on what often feels, especially for early stage or start-up companies, like a task with no clear bottom-line return. Nevertheless, it is crucial to ensuring that the confidential intellectual capital of the business will be protected against disclosure to the company's competitors. Without a comprehensive program in place, the chances of having a court take action to protect confidential information from disclosure to competitors is significantly reduced.

*I would like to thank Attorney Douglas G. Verge for his helpful advice and comments on this article.*

**This article is intended to serve as a summary of the issues outlined herein. While it may include some general guidance, it is not intended as, nor is it a substitute for, legal advice. Your receipt of Good Company or any of its individual articles does not create an attorney-client relationship between you and Sheehan Phinney Bass + Green or the Sheehan Phinney Capitol Group. The opinions expressed in Good Company are those of the authors of the specific articles.**