Implementing a Trade Secrets Protection Program

Insights
11.02.13

In the business world, protection of trade secrets can make the difference between success and failure, or profit and loss.This post seeks to show you how to protect your company's trade secrets so that in the event one of your employees steals a trade secret, you will be in the best possible position to succeed in litigation stemming from this theft.

How to Implement a Trade Secrets Protection Program
First, you need to identify your trade secrets (or perhaps more pointedly, the information for which you seek trade secret protection).The next step is to identify the specific physical, information technology and other security protocols your company can take to protect such information.The first line of defense against any form of corporate espionage is to implement a trade secrets protection program.This consists of a three-pronged approach: (i) addressing employment relationships; (ii) controlling access to your company's trade secrets; and (iii) knowing your company's employees.

A.Address Employment Relationships

i.Require Your Employees to Sign Confidentiality Agreements, Non-Solicitation Agreements, Covenants not to Compete, and Assignment of Invention Agreements
As a basic first step, to the extent permitted by applicable law, you should have your company's employees sign confidentiality agreements, non-solicitation agreements, covenants not to compete, and assignment of invention agreements.

A confidentiality agreement accomplishes four primary purposes: (i) it acknowledges that the employee has been or will be exposed to certain company trade secrets and other confidential and proprietary information; (ii) it identifies this information with at least some degree of particularity; (iii) it prohibits unauthorized use or disclosure of this information; and (iv) it requires the return of all trade secrets and other confidential and proprietary information on separation from employment and requires employees to sign a termination certificate declaring that all trade secrets have been returned.

A non-solicitation agreement prohibits a departing employee from soliciting, directly or indirectly, the company's customers or clients, regardless of where they are located, to do business with the employee.The primary requirement for a non-solicitation agreement is to identify the customers or clients that an employee cannot solicit.As a general rule, courts do not require that a specific geographical territory be included in the agreement, although various states do differ on this

geographical territory be included in the agreement, although various states do differ on this issue.In addition, when determining whether a non-solicitation agreement is reasonable, courts will often consider the extent to which the employee had actual contact with the customers or clients.Some states, like Louisiana, are more restrictive and require that, in order to be enforceable, a non-solicitation agreement must contain certain language required by statute.

A covenant not to compete – also known as a "non-competition agreement" or "non-compete agreement" – protects two aspects of corporate life: (i) customers or potential customers, and business interests that a company has spent considerable effort developing and which are vital to its financial health; and (ii) confidential information, which, if possessed, used or disclosed to unauthorized third parties could result in significant financial harm to the company.Most courts will enforce covenants not compete, as long as they are drafted in accordance with state law.As a general rule, covenants not to compete are enforceable only to the extent that they protect the legitimate business interests of companies (such as protecting trade secrets) and they contain reasonable time and territory restrictions.To be reasonable as to territory, a covenant not to compete should at most only address that territory which the company actively conducts business (although it is safer to restrict the territory to that in which the employee was actively engaged).To be reasonable as to time, a good rule of thumb is that most courts will enforce restrictions up to two years; three to four years will be closely scrutinized and held to a more rigorous standard; and five years or more will be virtually unenforceable (except perhaps in a sale of business context).

An assignment of invention agreement is a provision or separate document that "assigns" to the company any inventions or new discoveries made by an employee or independent contractor during the course and scope of his or her employment or work for hire.Some states, such as California, regulate the use of assignment of inventions agreements by requiring certain notice to employees (Lab. Code § 2870).

ii.Implement Appropriate Security Policies

Second, implement policies, to be signed by all of your company's current employees and new-hires, addressing the following areas: (i) the use of computers, e-mails, voice mail and the internet; (ii) physical access to trade secrets; (iii) telecommuting; (iv) employee privacy concerns; and (v) vendors and third party access to confidential information.

iii.Train Your Company's Employees

Third, train your company's employees and new-hires annually in basic security awareness, the company's security policies and procedures, their security responsibilities, and the proper procedures for reporting and dealing with theft of trade secrets.

Furthermore, consider including in the employees' personnel files documents that show the steps taken to inform him or her about the confidentiality obligations – such as a copy of the signed confidentiality agreement, receipt of the employee handbook and other key policies, a review of the

trade secrets protection program, and a record of attendance at training meetings that address the need to protect trade secrets.

iv.Protect Your Company's Trade Secrets Upon an Employee's Termination

Employee terminations create a particularly likely window for loss of trade secrets.Failure to take reasonable steps in the event of a termination can result in loss of critical information, or loss of trade secrets protection.In order to preserve your company's trade secrets, the termination or resignation of an employee with access to this highly sensitive information should trigger related security precautions.

You should immediately disable the accounts and access privileges of the terminated employee, and change all passwords, remote access codes, and, in appropriate instances, even VPN and dial-in numbers immediately at the time of termination.Also, you should "unplug" terminated employee's computer systems and remove dial-up modems from the terminated employee's workstation.Such actions will prevent the employee from accessing files after leaving.Examine the employee's computer/laptop before he or she leaves to determine if the employee has accessedand/or copied sensitive information in recent months.Conduct an exit interview and remind the employees during the exit interview of his or her continuing duty not to disclose trade secrets, and reference any documents to the effect.At the exit interview, request that the employee return all company property.Consider using a checklist for returning company equipment, keys and confidential information.You might also consider obtaining from the departing employee information about his or her new employer, which could help you determine the potential risk of any unauthorized disclosure or use of trade secrets.

B.Control Access to Your Company's Trade Secrets

Controlling access to your company's trade secrets means keeping the trade secrets confidential and providing access only to those having a legitimate need for it.This is especially important in protecting trade secrets because one or more critical elements of proof under most state laws is showing that steps were taken to protect the secrecy of the information.

i.Secure the Physical Environment

Examples of how you can secure the company's physical environment include:

- Restricting access to servers, routers, and other network technology to those whose job responsibilities require access;
- Installing surveillance equipment to monitor access to servers and other critical systems;
- Keeping wire closets, server rooms, phone closets, and other locations containing sensitive equipment locked at all times;
- Keeping an inventory of the equipment and periodically check for missing equipment;
- Placing locks on computer cases to prevent hardware tampering;

- Locking file cabinets and offices that store sensitive information;
- Designating all documents containing trade secrets or confidential information as "confidential" and implementing procedures to help ensure that all documents deserving the "confidential" designation are appropriately marked when initially created;
- Cross-shredding all paper documents containing confidential information before trashing them;
- Securing all dumpsters and posting "NO TRESPASSING" signs; and
- Making sure all discarded magnetic media is erased;

While it is not necessary for your company to utilize every one of the above-mentioned protocols in order for information to qualify as a trade secret, your company's failure to take routine physical precautions may lead a court to deny trade secret protection.

ii. Manage Access to the Company's Computer System Resources

Examples of how you can manage access to the company's computer system resources include:

- Implementing passwords for all employees for access to all critical system resources;
- Making sure passwords are set up with multiple characters (including numbers and letters);
- Requiring employees to change their passwords at least every 60 days and preventing them from reusing old passwords;
- Periodically training employees in password selection and protection and training them not to tell their passwords to others;
- Implementing controls on employees' use of the internet, the sites they can visit, and the software they can download; and
- Monitoring and logging employees' internet actions.

iii. Secure the Company's Computer System and Network

Examples of how you can secure the company's computer system and network include:

- Keeping audit logs of all access requests to critical systems and sensitive information;
- Encrypting sensitive information;
- If the company's network is on the internet, using a firewall and auditing the servers for security holes on a regular basis;
- Making sure the system has all of the latest security patches and fixes installed;
- Making sure all floppy disks brought into the company are scanned for viruses before use;
- Backing up all workstations and servers at least weekly and storing backups offsite;
- Keeping a log of all backups, including backup date, backup locations, and the employee performing the backup;

- Periodically testing the backup system to ensure the ability to restore date if necessary;

iv.Protect Against Third Party Disclosure

Examples of how you can protect the company against disclosure of its trade secrets to third parties (such as independent contractors, vendors and suppliers) include:

- Training your company's employees not to discuss the company's trade secrets or confidential information around third parties;
- Instructing employees to report any repair people that show up without being called, and to not grant access to equipment until their identities are established;
- Requiring all visitors to wear visitor tags and be escorted at all times;
- Utilizing contract and licensing agreements that expressly state the parameters for using certain information, and that include restrictions on "reverse engineering" or disclosing that information during activities such as a contract bidding process;
- Utilizing confidentiality provisions in standard contracts with any subcontractors or suppliers; and
- Meeting with third parties to stress the need for confidentiality for certain projects or other situations.

C.Knowing Your Company's Employees

One of the best ways to protect your company's trade secrets is not to hire a thief in the first place. When hiring employees in sensitive areas, or who will have access to confidential information, you should do a thorough pre-employment screening of those individuals.You might also consider performing background checks on current employees, as long as those checks are done in accordance with applicable laws (such as the Fair Credit Reporting Act and analogous state laws).

In the broadest sense, the term "pre-employment screening" is shorthand for the process of assessing applicants for a company's particular job or category of job.The assessment is performed according to company policies, based upon the nature of the job category and applicable laws (such as the Fair Credit Reporting Act and analogous state laws), which are designed not only to reveal fully qualified applicants, but also to potentially weed out those employees who may end up stealing your company's trade secrets.The elements of a pre-employment screening may include the following: education and credentials verification; past employment references; criminal history; motor vehicle report; social security number trace; credit report; workers' compensation records; civil lawsuits; judgments, liens and bankruptcies; security clearances; and merchant databases.

Conclusion

The day is past when trade secrets can be adequately protected merely by requiring employees to execute confidentiality agreements, non-solicitation agreements and covenants not to compete.Such traditional contractual protections can be of critical importance as a deterrent and in increasing the

success in trade secrets litigation, but now companies must deploy an arsenal of modern electronic weapons and physical barriers to protect their trade secrets and retain their competitiveness.In today's increasingly complex electronic world, effective protection against hi-tech theft must include proactive and reactive weapons.Without them, companies may have little chance of protecting the information upon which their business depends.

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either follow Michael R. Greco on Twitter or on LinkedIn or subscribe to this blog's RSS feed.

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email