

From the editors at
Clement Communications

Smart Supervision™

"Statistics drawn from various industry sources show that losses due to trade secret theft are estimated at more than \$150 billion a year."

STRATEGIES, IDEAS AND TIPS FOR MANAGING YOURSELF AND OTHERS

How To Implement A Trade Secrets Protection Program

By Ron S. Brand, Fisher & Phillips LLP

In the business world, information can make the difference between success and failure. It is estimated that 70 percent of the value of an average business is held within its information systems. Statistics drawn from various industry sources show that losses due to trade secret theft are estimated at more than \$150 billion a year. Despite the significant risk corporate espionage poses to companies, few companies spend the money needed to secure and protect their trade secrets from disgruntled employees.

The first step in assessing whether a company is adequately protected, or in increasing the protections that are in place, is to determine which company information is legally and practically protectable. Under the Uniform Trade Secrets Act, which many states have adopted with various twists, a trade secret is defined as follows:

Information, including a formula, pattern, compilation, program, device, method, technique or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Steps To Implementing A Trade Secrets Protection Program

Once a company's trade secrets have been identified, the next step is to pinpoint the specific physical information technology and other security protocols the 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 the company's trade secrets; and (iii) knowing company employees.

As a basic first step, employers should have company employees sign confidentiality agreements, non-solicita-

tion agreements, covenants not to compete and assignment of invention agreements.

A confidentiality agreement accomplishes a variety of goals, the most important of which is that it acknowledges that the employee has been or will be exposed to certain company trade secrets and other confidential and proprietary information.

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. 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.

Simply stated, a covenant not to compete prohibits a departing employee from working for a competitor for a certain period of time within a certain territory. Many courts will enforce covenants not to 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.

Second, implement policies, to be signed by all 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) vendor

(continued on page 2)

In This Issue

How To Implement A Trade Secrets Protection Program	1
Beating Procrastination In The Workplace	3
Are You Getting Your Message Across?	3
How To Praise Your Staff Effectively	4
Introducing New Technology To Workers	4
The Benefits Of Eliminating Performance Reviews	5
Flexibility For Working Fathers	5
Dealing With Change: What You Should Know	6

...and much more!

“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.”

How To Implement A Trade ...

(continued from page 1)

and third party access to confidential information.

Third, train company 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.

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. Reasonable steps include immediately disabling the accounts and access privileges of the terminated employee; changing all passwords, remote access codes, and, in appropriate instances, even VPN and dial-in numbers immediately at the time of termination; examining the employee's computer/laptop to determine if the employee has accessed and/or copied sensitive information in recent months; and reminding the employee during the exit interview of his or her continuing duty not to disclose trade secrets or reference any documents to that effect.

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

Securing The Physical Environment

Some examples of how to secure the company's physical environment include:

- ✓ Restricting access to servers, routers and other network technology to those whose job responsibilities require access
- ✓ Keeping wire closets, server rooms, phone closets and other locations containing sensitive equipment locked at all times
- ✓ 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.

Managing And Securing Access

It's also important to know how to manage access to the company's computer system resources, including implementing passwords for all employees for access to all critical system resources; and monitoring and logging employees' Internet actions.

In addition, secure the company's computer system and network by keeping audit logs of all access requests to critical systems and sensitive information. If the company's network is on the internet, use a firewall and audit the servers for security holes on a regular basis. Make sure the system has the latest security patches and fixes installed, and that all workstations and servers are backed up at least weekly, storing backups off-site. Also, ensure that the backup system is periodically tested to ensure the ability to restore data if necessary.

Perhaps equally important is knowing how to protect the company against disclosure of its trade secrets to third parties (such as independent contractors, vendors and suppliers). Some tools include training employees not to discuss the company's trade secrets or confidential information around third parties and utilizing confidentiality provisions in standard contracts with any third parties.

When hiring employees in sensitive areas, or who will have access to confidential information, do a thorough pre-employment screening, including performing a background check in accordance with applicable laws.

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. Without them, companies may have little chance of protecting the information upon which their business depends. ■

ABOUT THE AUTHOR

Ron S. Brand is a partner with the management-side labor and employment law firm of Fisher & Phillips LLP (www.LaborLawyers.com) in its Irvine, Calif., office. With a focus on both preventive counseling and defense of claims, the firm addresses the business and legal objectives of employers in a way that optimizes its clients' performance in today's changing marketplace. Brand can be reached at rbrand@laborlawyers.com. ■