This Alert focuses on the growing problem of trade secret theft by use of digital technologies, and suggests practical steps companies may take to implement trade secret protection programs to reduce their risks of being victimized by unscrupulous employees or outsiders.

In the bygone era of paper documents kept in file cabinets, theft of trade secrets often involved gaining access to locked rooms or files, making photocopies of numerous pages of documents, and removing those copies from a company’s premises. All of these steps involved some risk of being noticed by other persons in the workplace.

In the digital age, many documents exist electronically in several locations within a company’s computer system. Many companies allow their employees to have broad access to information on company Intranets. Departing employees who intend to go to work for competitors may be able to e-mail trade secrets contained in electronic documents to personal or other e-mail addresses, to copy enormous volumes of trade secrets onto CDs, or to walk off with laptops containing valuable information. Sophisticated outside hackers may be able to gain access to trade secrets by gaining unauthorized access to computer systems. Misappropriation of electronic documents may be hard to detect because employees wrongly copying data may appear to be quietly working on their computer.

Any employer that provides its employees with e-mail, access to a computer network, or laptop computers should guard against the digital theft of trade secrets. A recent computer crime and security survey revealed that 86% of the respondents experienced some form of attack on their computer systems from a “disgruntled employee,” in many cases causing employers to suffer significant monetary losses from unfair competition. (2003 Survey, Computer Security Institute/FBI Computer Crime and Security.)

It can be difficult to imagine your current employees engaging in such theft. However, there are numerous high-profile cases in which employees have done exactly that. The Department of Justice’s Computer Crime and Intellectual Property Section (CCIPS) website (http://www.usdoj.gov/criminal/cybercrime) lists examples where former employees have been criminally prosecuted for stealing their employer’s trade secrets – a federal crime punishable by up to ten years of prison and a fine of $250,000. In one recent case, a company’s information technology specialist pled guilty to trade secret theft after stealing a laptop computer and hard drive containing his employer’s trade secrets, and offering to sell them to a competitor for $3 million. It would be a mistake to assume, however, that only information technology specialists and hacker masterminds engage in the digital theft of trade secrets. In another case listed at the CCIPS website, for example, a service technician for a metal shredding equipment company pled guilty to downloading thousands of his employer’s closely-held trade secrets on the eve of his departure.

We advise our clients to protect their valuable confidential information with a trade secret protection program.

WHAT ARE TRADE SECRETS?

Misappropriation of commercially valuable confidential and proprietary business information is prohibited by the Uniform Trade Secrets Act (UTSA). Most jurisdictions in the United States – including the District of Columbia, Maryland, and Virginia – have adopted some version of the UTSA.

The Virginia Uniform Trade Secrets Act (VUTSA), contains a typical definition of “trade secret,” which is as follows:

(l) information, including but not limited to, a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) 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

(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
Examples of trade secrets may include drawings, blueprints, training manuals, laboratory notebooks, marketing strategies, financial and accounting information, manufacturing techniques, source code, recipes, data compilations, and product-development information.

Pursuant to the VUTSA, available remedies include: (1) an injunction prohibiting the use or disclosure of trade secrets, (2) payment of a royalty in exceptional circumstances, and (3) compensatory damages and exemplary damages, in certain cases. Moreover, a court is permitted to award attorney's fees to the prevailing party where, among other things, the misappropriation was willful and malicious.

OVERVIEW OF A TRADE SECRET PROTECTION PROGRAM

A trade secret protection program is a vital tool that companies can use to protect themselves from unfair competition by former employees and/or third parties. In the event litigation becomes necessary, a thoughtfully designed and well-implemented trade secret protection program makes it easier for the employer to convince a court that it has taken reasonable measures to protect their trade secrets.

Such programs typically include an information technology component, a human resources component, and a legal component. The information technology component may include:

- Establishing sufficient computer network security;
- Restricting and monitoring access to confidential information (i.e., password protection, limited access to highly confidential information); and
- Conducting periodic trade secret audits, including monitoring unusual computer or e-mail usage.

The human resources component may include:

- Establishing and enforcing an effective e-mail and computer user policy which notifies employees that their usage of those business tools may be monitored;
- Educating and reminding employees of their obligation to protect confidential information and other obligations with respect to the employer's employees, customers, and third parties;
- Restricting non-employee access to company property;
- Implementing post-employment procedures (e.g., exit interviews) to ensure that departing employees return all company property prior to leaving the premises, and to remind them of their post-employment obligations (e.g., maintaining secrecy of confidential information);
- Reviewing unusual computer or e-mail usage in the last month(s) of employment when companies learn of employee departures; and
- Requiring employees to sign restrictive covenants, including non-disclosure agreements.

The legal component may include:

- Reviewing materials disseminated to the public (e.g., marketing materials) to ensure that trade secret information is not publicly disclosed;
- Using confidentiality agreements with vendors, contractors, partners, and other third parties to whom the employer discloses the trade secrets, or other confidential and/or proprietary information; and
- Identifying trade secrets and appropriately marking documents and materials containing trade secrets.

Rapid changes in technology – coupled with the high turn-over rates in today's job market – require that an employer's information technology, human resources and legal departments communicate on a regular basis to ensure that the trade secret protection program is updated to reflect changes in technology, personnel and the law. Creation of a Trade Secret Protection Committee comprised of representatives of the information technology, human resources and legal functions may be appropriate.
CONCLUSION

If you are interested in more information on this subject, on February 13, 2004 at 2:00 p.m. (ET) Shaw Pittman partner Daniel P. Westman will be presenting a webcast entitled “Preventing Trade Secret Theft in the Digital Age” for the Information Technology Association of America. Registration for this webcast is free. You may register at http://www.itaa.org/isec/events/event.cfm?EventID=890.

Shaw Pittman has extensive experience counseling clients regarding trade secret protection programs, and litigating trade secret cases. For more information about these issues please contact:

Christine N. Kearns 202.663.8488
christine.kearns@shawpittman.com

Paul F. Mickey, Jr. 202.663.8233
paul.mickey@shawpittman.com

Joyce L. Oliner 202.663.8178
joyce.oliner@shawpittman.com

Daniel P. Westman 703.770.7616
daniel.westman@shawpittman.com