

Protecting Corporate Trade Secrets in a Digital Network Environment

FRANCIS J. BURKE JR. AND TYSON Y. WINARSKI

The value of corporate America's intangible property holdings is surging. The days where a company's net worth is primarily determined by its tangible assets have faded into history. Prior to the emergence of our modern, information-based economy, tangible assets accounted for 70 percent of corporate wealth, with a mere 30 percent of corporate wealth coming from intangible assets. Today, tangible assets account for less than 15 percent of corporate wealth. More than 85 percent of corporate wealth is now based on intangible property, such as patents, copyrights, trademarks and trade secrets. Of these four forms of intangible property, trade secrets are unique among them.

The U.S. Patent and Trademark Office and the U.S. Copyright Office provide registrations for those who wish to protect their inventions, trade identifiers and writings. The most substantial step a company can take toward protecting an invention, trade identifier, or writing is to apply for one of these registrations. Trade secrets are different. There is no federal agency delegated to register trade secrets. Protecting trade secrets requires a dogged and determined effort by cor-

porations in dealing with their employees, customers, contractors, licensees, joint venturers, consultants, outsourcers and other vendors. In the digital network environment that pervades corporate America, protecting a corporation's trade secrets to preserve enterprise value takes on a whole new level of urgency. For those corporate counsel charged with protecting these trade secrets, here is a road map for trade-secret protection in a digital network environment.

TRADE-SECRET LAW HELPS THOSE WHO HELP THEMSELVES

Does your company have a written trade-secret policy in effect? Information that is valuable and not generally known in the industry can lose its trade-secret status if the company does not treat the information as confidential. Put differently, in the trade-secret arena, the law helps those who help themselves. The Uniform Trade Secrets Act (UTSA) requires the use of "efforts that are reasonable under the circumstances" to maintain the secrecy of information. Reasonable efforts to maintain secrecy include advising employees and

Francis J. Burke Jr. is a partner in the Phoenix and Los Angeles offices of Steptoe & Johnson LLP. His practice emphasizes complex civil and criminal litigation and trials including individual, multiparty and class-action claims. He can be reached at fburke@steptoe.com. Tyson York Winarski is an associate in the Phoenix office of Steptoe & Johnson LLP, where he is a member of the Technology Department. He can be reached at twinarski@steptoe.com. The authors wish to thank Mark Kisicki and John Nickerson for contributing their trade-secret expertise toward editing this article.

block access to popular IM sites, such as Google's, and periodically scan your system to detect IM use. IM management solutions are available from IMLogic, WiredRed or Akonia.

Web Pages

Web pages are another potential source for leakage of trade secrets. Do you know what is posted on your Web site? Do your marketing department, Web design team, Web content manager and web hosting service know what information is confidential and should not be placed on the Web site? Companies can intentionally or unintentionally place confidential information on their Web pages, including customer lists and customer information, employees who are members of key product teams, product specifications, business plans and even portions of computer source code. Trade-secret owners should take great care in examining the information that is placed on their Web site. Further, web site owners may wish to consider restricting access to portions of their Web site through means of digital locks, password protection plans, other access control measures or at a minimum, some sort of click-through confidentiality agreement.

Chat Rooms, Message Boards and Blogs

Chat rooms and message boards can provide an effective means for communication between your employees, particularly when they are dispersed over different geographic locations. Who has access to your company's chat rooms and message boards? Your employees may be discussing or posting trade-secret or other sensitive information in these digital forums without your permission. Make sure to restrict and control access to company chat rooms and message boards. Implement a

trade-secret policy for use of chat rooms and message boards. Have your company computers keep a digital log of chat and message board sessions by tracking who and when your employees log on. Keep unauthorized persons from accessing your chat rooms and message boards with digital locks, password plans, other access control measures, or other means. Also, for those employees who regularly use and rely on the Internet for information, make sure to educate them to not discuss or post trade-secret or other sensitive information on non-company chat rooms or message boards.

Web logs, or "Blogs," are a new forum for public expression in cyberspace. Blogs typically consist of personal Web pages, message boards, and e-mail groups, where individuals express their

views in cyberspace. Although these blogs may discuss sports, politics or other subjects, it is not uncommon for employees to have blogs that comment upon their employer, or its management, products, services, competitors or industry. What trade secrets, confidential know-how or other sensi-

itive information is that employee disclosing when he or she discusses his or her employer in cyberspace? Under the UTSA, disclosure of trade secrets in an employee's blog would constitute misappropriation. Further, disclosure may also constitute a violation of a written nondisclosure agreement.

To prevent disclosure of trade-secret information in a blog, make sure to include prohibitions against employees posting confidential information on Web logs, chat rooms, discussion groups or other cyberspace forums, and make sure to have a written trade secret/confidentiality/nondisclosure agreement in place. Further, take active steps to search for and remove employee blogs on the Internet that disclose trade-secret information. A variety of search engines exist specifically search-

Who has access to your company's chat rooms and message boards? Your employees may be discussing or posting trade-secret or other sensitive information in these digital forums without your permission.

others of the existence of trade secrets and other know how, limiting access to trade secrets on a “need to know” basis, and controlling plant or onsite access. Reasonable uses of a trade secret, such as controlled disclosure to employees and licensees, is consistent with such efforts to maintain secrecy under the UTSA.

STICK WITH TRADITION

In a digital network environment, it is important to practice traditional efforts to protect trade secrets. You must restrict access to those who need to know the information and require those persons to enter into trade secret/confidentiality/nondisclosure agreements. Make sure to identify and mark documents and electronic information that contain trade secrets or confidential know-how as “Confidential: For Internal Use Only.” Do not distribute documents or electronic information marked as confidential to just anyone. Limit distribution of confidential documents or electronic information to those on a “need-to-know” basis. Do not dilute and weaken your assertion of confidentiality over a document or electronic data containing trade secrets or confidential know-how by liberally applying the label “confidential” to all company documents or digital information, such as e-mails to co-workers asking what restaurant everyone would like to go to for lunch on a given day. Create a companywide confidentiality policy that is distributed at least annually to all employees and on the date of hire for new employees. Require all employees to execute a trade secret/confidentiality/nondisclosure agreement. Require all contractors, licensees, joint venturers, consultants, outsourcers and other vendors with access to trade secrets or other confidential information to sign a trade secret/confidentiality/nondisclosure agreement and require that they get such agreements signed by any third parties to which they may disclose the information. Further, provide means by which employees can report improper use of company trade-secret information to management.

LOOSE LIPS SINK SHIPS

Keeping control of trade-secret information is essential to protecting it. Maintain records of persons to whom trade secret information is made available, when the information is released and returned, and the nature of the trade secret. Establish security measures on the business premises that include sign-in procedures, badges, restricted access for visitors and employees, and locks or other access control measures on computers, digital storage media, cabinets or rooms containing sensitive information. Do not allow cell phones, cameras or other recording devices into your premises that contain trade-secret information and establish a procedure for checking any digital storage media exiting your premises.

THE REVOLVING DOOR

Your departing employees and those of your vendors are a constant potential source for losing control of trade-secret information. As they leave the company site, so does all of your trade-secret information that is contained in their minds, USB drives, memory sticks, CDs, DVDs and any other electronic or paper information in their possession. Stemming this trade-secret leakage begins with an inventory of items prior to employee departure. Schedule exit interviews with all departing employees. In the interview, remind employees of their continuing obligation to maintain secrecy of company information; collect all confidential documents, electronic information and digital storage devices that are in their possession, and make sure to follow up the interview with a letter to employees reminding them of their obligations.

ENTER THE DIGITAL NETWORK ENVIRONMENT

The digital network environment brings added challenges to those charged with protecting corporate, trade-secret information. In a digital network environment, there are four primary areas where

trade secrets are put at risk: e-mail, Web pages, chat rooms, message boards and Web logs, and digital information storage.

E-Mail

In 2002, e-mail users sent more than 31 billion e-mail messages globally on a daily basis. On average, 2002 e-mail users handled 61 e-mail messages per day. In 2003, e-mail users received an average of 110 e-mails per day. In 2005, it is expected that individuals handle more than 300 e-mail messages per day. By 2006, it is estimated the e-mail users will send 60 billion e-mail messages on a daily basis. More than half of those e-mails will be person-to-person e-mails, with the remainder consisting of spam. A recent study by ESG research estimates that 70 percent of an organization's intellectual property resides within its e-mail system. With billions of e-mails travelling the globe at the speed of light, with little more than a mouse click to set them loose, how many will contain your company's trade secrets?

Corporate employees may intentionally or unintentionally destroy the confidentiality of trade-secret information by transmitting it to others. Employee education is key to stemming trade-secret leakage in a network environment. A first step is to adopt a confidentiality plan that is made known to employees. Make sure to impress on your employees the significance of providing unprotected confidential information to others outside the company. If it is necessary to share confidential information with vendors, get those vendors to enter into confidentiality agreements. Distribute an e-mail policy informing employees that any e-mail that passes through a company

computer is considered company property and may be monitored. Further, companies should have a policy prohibiting the forwarding of any company document or electronic information that contains trade secrets or confidential know-how to an outside e-mail account without prior supervisory approval.

Taking physical steps to block the transmission of e-mails containing trade secrets is another crucial method to protect your intellectual property. A category of e-mail compliance and archiving software exists that serves as an add-on to

Microsoft Exchange and Lotus Notes. These compliance software modules can search and block the transmission of suspicious e-mail, based upon the inclusion of search words in the e-mail that are selected by the employer. Although the use of this software requires the development of a word search vocabulary to identify suspicious e-mails that would indicate disclosure

of trade secrets, the software has wide applications in terms of Securit and Exchange Commission (SEC) compliance, data security, and intellectual property security. Vendors in this category include iLumin, C2C, Legato, KVS and Zantaz.

Instant messaging within corporations is exploding in popularity and is often used to circumvent corporate security and information retention programs. Instant messages (IMs) can carry trade secrets and transfer digital files right out of your company. The threat of trade-secret leakage through IMs has greatly increased now that Google has added an instant messaging service, available at <http://www.google.com/talk>. Unless you are prepared to implement a full-scale IM management solution, your policy manuals should ban the use of IMs on your system, you should

A recent study by ESG research estimates that 70 percent of an organization's intellectual property resides within its e-mail system. With billions of e-mails travelling the globe at the speed of light, with little more than a mouse click to set them loose, how many will contain your company's trade secrets?

ing blogs, such as Technorati's blog search engine available at www.technorati.com, Feedstar at www.feedstar.com, and Blogdigger at www.blogdigger.com. Google has also launched its own blog-specific search engine, currently in beta testing, available at blogsearch.google.com.

Digital Information Storage

In a digital network environment, all of your corporate data, electronic documents, spreadsheets, presentations, e-mails, electronic files, chat room discussions, message board postings and other electronic information is stored in a digital file in some form of digital storage media. These may range from personal computer storage media, such as hard drives, floppy drives, CDs, DVDs, USB drives or memory sticks, to server or mainframe hard drives, disk drives, tape, optical drives, and an ever increasing number of mass storage devices and architectures. How are you protecting those files and digital information?

Network intrusion protection and data security is important to both identity theft and intellectual property theft. Network intrusion perimeter security is essential. Make sure to electronically label your digital trade-secret information with a confidentiality identifier. Use electronic locks, passwords, other access control devices, warning screens, encryption, coding, or shrink warp and license agreements to control access to your information. Encrypt all e-mails that go outside the company and also encrypt data that is stored on backup tapes and other storage media. Several recent, highly publicized incidents involving loss of sensitive personal customer data might have been avoided if those companies had encrypted their customer data that was stored on tapes that were subsequently lost. Control the physical access to your network. Is it really necessary to connect to the Internet a critical set of computers that stores the important trade-secret information?

Do You Know What Your Trade Secrets Are?

Most companies can readily point to their patent portfolios and their lists of registered trademarks and registered copyrights. However, many companies do not take the time to identify and log their trade secrets. A company cannot protect its trade secrets until it first locates, identifies and catalogues them.

As corporate wealth becomes increasingly dominated by intangible property, a robust, effective, and dynamic trade-secret protection program is necessary to preserve enterprise share value. Does your trade-secret program sit lifelessly in a memo contained in your employee manual, or is it something that is practiced and discussed regularly at your company? Employee and vendor education is key to protecting trade secrets. Trade-secret loss often occurs through inadvertent or accidental disclosure by your employees or your vendors' employees who were unaware that the information at issue contained trade secrets or other confidential know-how or that their actions inadvertently released trade-secret or confidential information. When employees and vendors know what a company's trade secrets are and how to handle and protect them, that company can stop much trade-secret leakage. The price of defending your trade secrets is eternal vigilance with your employees, contractors, licensees, joint venturers, consultants, outsourcers and other vendors.

TRADE SECRET PROTECTION CHECKLIST

- Robust, effective, and dynamic trade secret protection program is key
- Must be practiced and discussed regularly
- Employee and vendor education important
- Avoid inadvertent or accidental disclosure by employees or vendors' employees
- Price of defending trade secrets is vigilance with employees, contractors, licensees, joint venturers, consultants, outsourcers, and other vendors