SHEEHAN PHINNEY BASS + GREEN PA

ATTORNEYS AT LAW

Boston Concord Hanover Manchester

David W. McGrath
Direct dial: 603.627.8255
Fax: 603.641.2349
dmcgrath@sheehan.com

Author

Charles P. Stewart, Legal Technology Specialist

Practice Areas

Business Litigation

Good Company

Minimizing the Risk of Data Theft Through Cloud Computing

Tuesday, February 07, 2012

Imagine the following: Your business has a banner year, but when word leaks that sales staff will not be receiving the discretionary year-end bonus, one of your key sales employees decides to pursue an opportunity with a competitor. She knows that her customer and prospect information will be of great help to her, but she is also aware that the company's IT department has security measures in place that will alert them to downloading of files from her workstation. After spending just a few minutes on the web, she learns how to install a free app on her iPad that enables remote access to her work files. With the help of her new app, she surreptitiously copies to her iPad all of the confidential records she has accumulated for the last few years. Next, she meets with the sales manager of your biggest competitor and with the information on her iPad entices her potential new employer. With offer letter in hand, she gives her notice and departs without your IT staff knowing that proprietary information has been taken from your secure network.

This type of security breach is becoming more common. In order to better understand the nature of this burgeoning technological threat, it is helpful to examine how we got to this point. When proprietary information was solely in paper form it was relatively easy to keep track of copies. The transition to electronically stored information and internet availability at work and home complicated tracking, but IT departments developed robust protocols and checks and balances to protect confidential and trade secret work product. Most companies today have secured their network behind a strong firewall and have thorough electronic information policies designed to limit the likelihood of rogue employees smuggling sensitive information out of the workplace on thumb drives, micro drives or just-burned DVDs. The threat today, however, comes from a new technology against which the security industry has yet to defend.

With the proliferation of smart phones and tablet computers, manufacturers created a new methodology of installing and storing software on these portable computing devices. The application, or "app" as it has come to be known, was revolutionary in that it allowed a single instance of a program to be installed on a device with a tiny software footprint on the device itself. The bulk of such programs' data is stored externally on remote servers, connected to the device by a wireless or cellular signal. This type of remote storage of software is known as "Software as a Service" (SaaS), and storage of the software is said to be "in the cloud". This data storage technology in the past few years was revolutionary in the small electronic device evolution and allowed a handheld device to contain a large number of programs to be installed in a tiny amount of physical space, all for a much reduced cost.

For the software industry, cloud technology created a venue for a large number of small developers to create, test and distribute programs. The advance to the tablet computer (and we are discussing tablets that run on the Apple iOS platform or Android platform, not the notebooks computers that use a tablet format but run regular desktop software) was the next logical step for this type of technology and the app market exploded for both Apple's iOS and the Google's Android platform.

Tablet computers like iPads, however, needed to offer more than the smartphone; they needed to have business apps and work in collaboration with home or office computers easily. This connectivity and communication issue was solved by apps that synched files and folders with remote third party servers in "the cloud", which then made the files available to any computer connected to the internet anywhere in the world.

Apps like Dropbox, SugarSync, SpiderOak, Box.net, which perform this function, have become standard on portable tablet devices, and many developers now program their apps to be "Dropbox Compatible". Once installed on the user's computers and portable devices, Dropbox provides a folder where files may be placed and instantly shared with any other logged in instance of that dropbox.

While the proliferation of portable computing was instrumental to the development of this technology, it is important to note that one does not need a portable device to use this technology. An employee can have a program like Dropbox installed on their workstation in the office and someone across the globe with the program installed on their computer can have instant access to any file copied to the Dropbox folder. Files can be dragged to the Dropbox, left there for 15 minutes while they are copied remotely, and then dragged back to their original location without most IT departments ever being aware of the file transfer.

Dropbox, and programs like it, serve a valuable role in tablet computing, making available any number of files or documents to remote users without the users having to download the files to their portable device before working remotely. They also allow for remote collaboration between offices without an elaborate Wide Area Network connection or VPN tunnel. But the risk to proprietary and trade secret information has to be understood and acknowledged before employees are allowed to install these types of cloud storage programs on their work devices.

Today's new technology makes theft of proprietary and confidential information exceedingly easy for even basic computer users. While there are no sure-fire ways to inoculate against this kind of theft, there are some steps all companies should take to minimize their exposure, and the law offers some protection. Even if you have not followed one of our recommended best practices (see below) and do not require employees to execute non-disclosure agreements, your business can still protect its proprietary information if the information is considered a "trade secret". In determining whether information rises to the level of a trade secret under the law, there are two factors courts examine, which simplified are: (1) is the information readily ascertainable by legitimate means elsewhere, and (2) did the business take reasonable steps to keep the information confidential. Focusing on the second of these factors, the law basically requires employers to apprise their employees that there is an expectation that business information will be kept confidential; that the company considers the information to be the company's property and a trade secret; and that the information is important and cannot be shared with or disclosed to anyone outside the company.

Businesses should take basic steps to protect confidential and proprietary information, whether or not that information rises to the level of a trade secret. As has been suggested in past Good Company articles (see, e.g., April 2009 edition, Vigilance: The Watchword for Dealing with Employee Migration in "Hard Times"), businesses should (a) require incoming employees to sign, as a prerequisite of employment with the company, a non-disclosure agreement; (b) develop a written trade secret and confidential information policy, which advises employees to safeguard proprietary information; (c) educate employees about what information is deemed confidential and protected, and (d) remind departing employees at an exit interview about their post-employment obligations concerning the company's proprietary information.

So, with these basic but important best practices in place, what additional steps should a business take to defend against new age, electronic data theft? At this time, there is no sure fire way to block this technology beyond forbidding the installation of it on company assets through strict Group Policies put in place by your IT department. Of course doing this precludes, or at least severely restricts, use of tablet computer technology for all employees. Where this is not feasible or desired, here are some best practices for mitigating the threat.

- Practice the Principle of Least Privilege. Allow access to files based solely upon the need to use them. Develop robust Group Policies with your IT department that restrict access and rights to sensitive information.
- Short of using Group Policies and Windows Active Directory, have your IT Department assign read only attributes to sensitive or confidential information.
- Consider shared or group Dropbox accounts where unauthorized traffic might be more noticeable.
- Turn on RSS tracking on corporate Dropbox accounts which provides a log of all activity in RSS feed format.

This threat from the use of cloud services developed for the portable computing market is the latest in a dynamic, increasingly paperless, world. There will, no doubt, be some new technology next year, or the year after, that will threaten data security in a new yet unforeseen way. With strong policies and practices based on an understanding of the law and technology, businesses will be able to reduce the likelihood of trade secret and other proprietary information being pirated.