Bond
INFORMATION MEMO
INTELLECTUAL PROPERTY
AND TECHNOLOGY
APRIL 2016

Head in the Cloud: The Insider Threat to a Company's Trade Secrets

By Bradley A. Hoppe and Heath J. Szymczak
Reprinted with permission from the April 4, 2016 edition of the New York Law Journal

After months of searching, a client finally hires its "dream candidate." The client welcomes the new employee with open arms and wants to provide all the resources needed for the employee to succeed, entrusting the employee with access to its confidential information. Unbeknownst to the client, however, the new employee merely views the position as a stepping stone to something bigger. From day one on the job, he continues his job search, secretly reaching out to some of your client's biggest competitors (who also view him as a "dream candidate" partly because of his position with your client). A few months later, the honeymoon comes to an abrupt end when the employee puts in his notice that he is leaving for a new position with a competitor. The real shock is yet to come: when your client learns that its trusted employee has uploaded some of its most highly confidential competitive information (e.g., customer lists, pricing information, customer requirements, diagrams, specifications, manufacturing processes and formulae) to a thumb drive, personal email or, even worse, the cloud.

This nightmare hypothetical is all too common across all industries, yet many companies remain woefully unprepared. Perhaps as the result of the exposure by the media to the cybersecurity threats posed by outsiders, companies often overlook (and, in many cases, completely ignore) the more immediate and substantial threats posed by insiders, namely their own employees. Recent surveys of companies and their employees and analyses of trade secret cases in federal and state courts reveal the following startling facts: (1) trade secret thefts are on the rise, with the number of cases involving trade secret theft doubling between the years 1988 and 1995, doubling again between the years 1995 to 2004, and, at the current rate, likely doubling again by the year 2017;[1] (2) more than 85 percent of all trade secret thefts are believed to be perpetrated by an employee or business partner;[2] and (3) more than half of employees recently surveyed have admitted to taking information from their former employer and approximately 40 percent of those same employees acknowledged that they intended to use that information on behalf of their new employer.[3]

Despite these statistics and the significant threat posed by employee insiders, companies continue to grant employees nearly unfettered access to their trade secret information without any—let alone adequate—safeguards in place, often with disastrous and irreparable consequences to their business. This article will provide not only a general overview of the law of trade secrets, but also practical steps clients can take to better protect their information from the insider threat, as well as illustrative case examples of the consequences of failing to act.

What Is a Trade Secret?

Unlike most other states, New York has not adopted any form of the Uniform Trade Secret Act, but instead relies on the following common law standard, as set forth in the Restatement of Torts §757, comment b:

A trade secret is any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. In deciding a trade secret claim several factors should be considered: (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[4]

Simply put, a trade secret can be anything which gives a company a competitive advantage and, most importantly, is kept secret and confidential. Trade secret information can take many forms and, so long as it meets the above standard, can include product designs, formulae, manufacturing processes, financial data, customer lists, customer requirements and pricing, source code, market research, and business plans.

What Is the Biggest Threat?

Notwithstanding the time and resources clients often expend in developing valuable trade secret information, they remain vulnerable to the insider threat posed by their own employees.

It used to be that companies had to worry principally about the theft of physical files; this of course evolved as technology changed from the use of floppy disks, to CDs and DVDs, to the use of personal email accounts, to small USB based thumb drives to download and abscond with sensitive electronic files. Today, while some of these—thumb drives and personal email specifically—continue to be used by employees and present threats to our clients, they are far easier to prevent and detect than the potentially catastrophic threat posed by cloud computing generally and cloud-based storage specifically. These "USBs in the sky" allow an employee, who has access to commercially sensitive information and a personal cloud storage account through Dropbox, OneDrive, Google Drive, iCloud, etc., to upload trade secret and other confidential files to the "cloud."[5] Once on the cloud, an employee can and oftentimes does access, download and transfer to third parties his/her employer's trade secret and other commercially sensitive information. Not only can this cause significant and potentially irreparable harm to a client if the information falls into the hands of a competitor, but the fact that it can be disclosed to third parties and, in essence, made public, could very well deprive the client of the ability to obtain trade secret protection of that information down the road.

We are just now starting to see published cases coming out in state and federal courts involving the use of cloud computing for the purpose of misappropriating trade secret information. For example, in a case out of the Eastern District of Texas,[6] the defendant, plaintiff's former COO, utilized Dropbox on the day of her resignation to upload literally thousands of confidential patient files and other commercially sensitive trade secret files. Fortunately for that plaintiff, its former COO made an off-the-cuff comment to one of the plaintiff's human resource employees that "she knew where too many bodies were buried," which led the employer to conduct a detailed forensic investigation of the former COO's computer equipment. Had no such comment been made and no investigation conducted revealing the use of Dropbox, there is no telling the amount of damage that could have been done to this plaintiff's business.

Similarly, in a case out of the Eastern District of Michigan,[7] an employer came to learn that one of its former employees, at or around the time of his resignation, uploaded myriad commercially sensitive files to Dropbox. The plaintiff there immediately brought an application for a preliminary injunction seeking to prevent that former employee from not only using the information taken, but also continuing to operate his competing business. While the court granted the injunction with respect to the use of the information and required that the information be returned and his computer, other electronic devices and cloud and other storage applications scrubbed at plaintiff's cost, the court refused to enjoin operations of the competing business due to the absence of a non-competition agreement or strong evidence that the commercially sensitive information was actually accessed and used post-resignation. Not only does this case illustrate the need for companies to implement policies designed to detect the use of cloud-based storage applications, but also for the use of reasonable restrictive covenants (e.g., non-disclosure and/or non-competition covenants) with strong attorney fees and cost shifting provisions.

With new technologies being developed every day, it is imperative to advise clients regarding the risks presented by employees generally and the use of cloud-based storage and other means to abscond with information, as well as the steps that can and should be taken to help lessen the risk of theft and, in the event that an employee succeeds, detect any such theft in a timely manner.

Protecting Against Insider Threats

One of the best—and most common—ways to protect trade secret information, as well as the customer relationships and goodwill that an employer spends significant time and resources in developing, is through the use of reasonable restrictive covenants, such as non-disclosure, non-competition and/or non-solicitation provisions. Not only are restrictive covenants effective in preventing trade secret theft, but courts have made clear that where an employer fails to use such covenants, that employer cannot establish that it took reasonable steps to protect its information and thus have it recognized as "trade secrets" when forced to protect its rights in court.[8]

Where clients often get into trouble is that they try to restrict too much or use a "one size fits all" approach, both of which may subject the covenant to invalidation as overbroad or unnecessary to support a legitimate business purpose.[9] If used correctly and tailored to the particular employee and interest at stake (here, the protection against use and disclosure of trade secret information), a non-competition or other restrictive covenant can be one of the more effective tools in protecting against the theft or unauthorized use or disclosure of trade secret information, particularly when coupled with the additional deterrents of attorney fees and forensic cost shifting provisions. It must be noted, however, that courts everywhere—including New York—are increasingly suspicious of restrictive covenants as a condition of employment, either initial or continued; it is thus imperative that a client consult with counsel to draft and/or review their restrictive covenants prior to presenting them to their employees, particularly with the recent trend to invalidate entire covenants if there exists evidence of overreaching and/or coercion.[10]

In addition to the use of reasonable restrictive covenants tailored to the specific employee with access to trade secret information, clients must implement policies designed to protect their valuable information. Many clients, however, continue to grant certain of their employees, even those with no legitimate business reason, nearly unfettered access to what they consider to be their trade secret information. It is imperative for a client hoping to obtain trade secret protection from the courts to implement some combination of the following common sense policies:

- Limit access to trade secret information to only those employees who need it to perform their job responsibilities. Not only does this limit the universe of potential threats, but it also shows a court that reasonable steps were taken to protect information in the event that a theft occurs and protection is needed.
- Implement policies to address the use of cloud storage. With respect to personal cloud-based storage, it is recommended that clients not only prohibit the use of such storage applications, but work with their internal IT departments to disable the ability of employees to utilize them. In addition, where a client utilizes employer-based cloud storage, the client must ensure that proper safeguards are being used to monitor and track access, such as unique log-in credentials for each employee.
- Conspicuously designate confidential or trade secret documents so that employees are on clear notice as to how they should handle certain materials.
- Implement policies to monitor and track an employee's access to and use of trade secret information.
- Prepare written trade secret protection policies for access to and use of company information. Such policies should, at the very least, be distributed to, and reviewed and initialed by, any employee with access to trade secrets.
- Exit interviews. All clients should conduct an exit interview of all departing employees and, as a part of each such interview, remind that employee in writing of his/her contractual and common law obligations with respect to company information, post-employment obligations and prohibitions, etc.
- Collect and secure computers and electronic devices used by terminated employees. Computers and electronic devices need to be set aside in a secure place and, without exception, not placed back into circulation unless such computers and devices have already been imaged by a forensic consultant.

Lastly, given the significant risks posed by employees to a client's trade secret information and other intangible assets, it is advisable for clients to routinely have their policies and procedures, as well as their restrictive covenants, audited and updated to better ensure that they are in compliance with the ever-changing law and best practices. As any trade secret litigator (or any business owner forced to litigate a trade secret in court) will surely attest, the nominal cost to a client associated with such a periodic preventative audit pales in comparison to the costs associated with either the loss of a trade secret or litigation to protect and enforce trade secret and other related rights. As the old saying goes, an ounce of prevention is worth a pound of cure.

Endnotes:

1. David S. Almeling, Tracking Trade Secret Stats (2010).
2. David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum and Jill Weader, "A Statistical Analysis of Trade Secret Litigation in Federal Courts," 45 *Gonzaga Law Review* 291, 303 (2010).
3. Symantec Corporation, "What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk," at 1 (2013).
4. *Ashland Management v. Janien*, 82 N.Y.2d 395, 407 (1993) (quoting Restatement of Torts §757, comment b).
5. For those unfamiliar with the term, the "cloud" is best described as the use of a network of remote servers hosted on the Internet to store, manage and process data, as opposed to the use of a local server or a personal computer.
6. *Frisco Medical Center, L.P. v. Bledsoe*, 2015 U.S. Dist. LEXIS 159915 (E.D. Tx. 2015).
7. *PrimePay v. Barnes*, 2015 U.S. Dist LEXIS 65710 (E.D. Mich. 2015).
8. *See Delta Filter v. Morin*, 108 A.D.2d 991(3d Dept. 1985) (holding that in the absence of a nondisclosure agreement the plaintiff could not establish that the defendant used improper or wrongful means to obtain plaintiff's purported trade secret information); *see also Starlight Limousine Serv. v. Cucinella*, 275 A.D.2d 704 (2d Dept. 2000) (holding that information did not constitute trade secrets where the company failed to require the employee to execute any kind of agreement to keep the information secret or not use the information after leaving employment).
9. *See, e.g., BDO Seidman v. Hirshberg*, 93 N.Y.2d 382 (1999).
10. *BDO Seidman v. Hirshberg*, 93 N.Y.2d 382 (1999); *Scott, Stackrow & Co., C.P.A's, P.C. v. Skavina*, 9 A.D.3d 805 (3d Dept. 2004); *Gilman & Ciocia v. Randello*, 55 A.D.3d 871 (2d Dept. 2008); *Brown & Brown v. Johnson*, 115 A.D.3d 162 (4th Dept. 2014), *reversed on other grounds*, 25 N.Y.3d 364 (2015).

By Bradley A. Hoppe and Heath J. Szymczak