Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Oh, The Places IP Will Go: How To Prevent IP Theft

Law360, New York (October 07, 2013, 5:47 PM ET) -- This may be the 100th article you've read saying that companies' technology is as mobile these days as their employees and that employers must do more to protect their intellectual property. Yet, given how commonplace that observation is, it is surprising how few companies have taken a serious, fresh look at developing the right legal agreements and investigative protocols to protect their most valuable intellectual assets.

Active prevention of IP theft is a two-step process. First, companies must take a more thoughtful approach to their employment agreements and must be willing to jettison age-old concepts in favor of active contract language that gives an employer visibility into the ways an employee may have stolen IP and access to the places where an employee may have downloaded or stored it.

Second, companies must design policies and procedures to more actively mitigate the risk of IP theft and limit corporate exposure when it does occur.

Designing Employment Agreements with Reality in Mind

Restrictive covenants that require an employee to not misappropriate an employer's property are literally centuries old and developed well before electricity, let alone electronic information. Most employers still use employment agreements drafted from these old habits, requiring their employees to "return" all "property."

That may have been effective when most intellectual property was tangible: An employer generally knows when a physical file folder, a hard-copy memo or a blueprint has been returned. But how do you "return" an email that your iPhone downloaded off an exchange server and now lives in a "cloud?"

Restrictive covenants must evolve to cope with the transformed way employees access, store and share company information. In essence, a good restrictive covenant will rely less on an employee "doing the right thing" and more on giving a company a broad ability to determine how an employee may have intentionally — or even inadvertently — taken information, as well as to inspect all the locations in which the information might be stored.

A more effective covenant will expressly state that the employer has the right to the following:

- Maintain a record of, and require an employee to affirmatively identify, all electronic devices (whether personal or company-issued) on which an employee views, downloads or stores company information of any kind

- Inspect upon demand any electronic device that an employee may have used to view, download or store company information, regardless of whether the device is personal or company-issued: Here, the agreement should state that an employee can't raise a privacy concern as a way of shutting down an employer's inspection

- Require an employee to make any device available for immediate inspection and expressly agree that an employer is entitled to immediate injunctive relief to get the device if the employee does not cooperate

- Inspect upon demand all devices that information may have traveled to, not just the "initial" device: For example, a sensitive PDF file in a company email may be uploaded to a personal smartphone. From there, the same email may be forwarded to a private email account. And from there, the PDF may be saved to the hard drive of a personal PC. It's the PDF file we care about, so the employer needs the right to look at the smartphone, the email account and the personal PC –- otherwise, the employee can evade the ultimate purpose of an inspection, which is to figure out if they retained a copy of the PDF.

Including these specific protections in employment agreements makes it easier for a former employer to point to a specific breach of contract and gain immediate access to necessary devices and files when an employee refuses to comply. This is particularly relevant when time is of the essence. Take the following two cases.

Case One

A senior sales professional at a leading office furniture design company left to take a similar position with one of the company's main competitors. As a company leader, he had access to critical sales information and business plans.

The sales professional had signed a restrictive covenant that expressly granted the right to inspect any electronic device at the time of departure and to delete stored IP. He allowed the company to begin an inspection but cut it off when he became uncomfortable, claiming that he didn't want the company to look through his personal information.

Unfortunately for him, his employment agreement gave the company broad rights to examine personal devices and entitled the company to immediate injunctive relief to compel compliance. With a court order in hand, the company did a deep dive into his devices, found much had been misappropriated and prevented future disclosure of its confidential information to a major competitor.

Case Two

In a second case, a weaker agreement led to dramatically different results. A top designer at a luxury brand left her employer for a competitor. She had signed a standard employment agreement at the time of hire with age-old, nonspecific return-of-property language requiring only that she return "all company property" upon her departure. Her former employer had no immediate right of access to her personal devices, so the company had to resort to protracted litigation to get access.

The employer knew that the employee had stolen confidential information because the effects of the theft were already being felt in the marketplace, but winning a limited right to review the former

employee's personal devices took four months. The company ultimately found on the personal devices exactly what the former employee left there for them to find: nothing.

While both companies had restrictive covenants in place, the office design company succeeded in preventing its IP from leaving the company, thanks to a clearly defined right to aggressively and immediately seek out its own confidential information. Conversely, the well-worn language of generic covenants used by the luxury brand did not help the company prevent IP theft.

The right contractual protections fit hand-in-glove with developing the right investigative policies and procedures to protect IP.

Developing Investigative Protocol to Prevent and Demonstrate Employee Breaches

While critical, restrictive covenants are only as strong as an employer's ability to demonstrate that a breach of contract by an ex-employee has occurred. Therefore, it's important that legal counsel is able to work closely with information technology and forensic professionals when a company suspects its proprietary information has been stolen.

There are several investigative measures that can be taken to identify possible culprit(s) in an effort to contain or mitigate potential damages, including the following.

Defining an Investigative Protocol

Before a breach ever occurs, employers need to have a clearly defined and documented investigative protocol in place, which identifies the parties that should be involved (counsel, IT, forensic professionals) and outlines the steps that must be followed to quickly reach a resolution.

It's also important that companies have fully briefed all relevant parties to ensure that they're ready to work in concert to quickly figure out who took the company information, when it was taken, where it was located and how to get it back — or at least how to remedy any damage ensuing from its theft.

To prevent future thefts or leaks, companies should also conduct frequent system evaluations to identify possible weak areas and make the required improvements.

Performing Forensic Analysis before the Evidence Is Gone

Once a breach has occurred, companies must act quickly. To avoid losing or possibly contaminating evidence that points to who stole the company information and where it may be located, computer forensics should be conducted by certified forensic specialists as quickly as possible.

Most forensic information is not readily apparent to internal IT professionals or typical end-users. Forensic specialists, however, can uncover revealing user activity in connection with a theft by reviewing connected computing devices and detecting deleted files or Internet-browsing activity to identify suspects or stolen material.

Conducting Employee Interviews to Provide Supplemental Information

Employee interviews are another important step in the investigative process. Speaking with co-workers of an employee suspected of misappropriating corporate IP can yield critical, supplemental information

on the facts and circumstances surrounding the breach.

Combined with the data gleaned from computer forensics analyses, employee interviews can enable counsel and forensics professionals to determine “who was at the keyboard” at the time an incident took place.

Protecting the Company

Protecting corporate IP has become crucial for any organization operating in today’s electronic age. A well-planned investigative process for responding to incidents of data theft can go a long way to minimize potential damage and limit further losses.

Combining a cogent investigative plan with effective legal tools, such as comprehensive restrictive covenants, will enable employers to get their IP back and thereby limit corporate exposure.

--By Michael Barba, BDO Consulting, and Mark Konkel, Ford & Harrison LLP

Michael Barba is a managing director in the New York office of BDO Consulting with experience in domestic and international investigations involving high-tech crime, misconduct and network security matters.

Mark Konkel is a partner in the New York office of Ford & Harrison. He advises clients on employment law compliance, best employment practices, employee hiring and termination, protection of intellectual property, restrictive covenants and business expansions and reductions-in-force.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.