LATHAM & WATKINS LLP

DISCUSSING THE TRENDS

Q&A with Perry J. Viscounty

Trade Secret Protection Plans: Guarding Against IP Theft

January 15, 2014

The theft of intellectual property poses a significant threat to American companies. Perry Viscounty, a partner at Latham & Watkins and Chair of its Orange County Intellectual Property Group, is well versed in the potential pitfalls that can leave companies vulnerable to unauthorized disclosure of their sensitive information. In this Q&A interview, Viscounty offers advice on how companies can preemptively protect themselves from trade secret theft by insiders and outlines the steps that should be considered if confidential information is stolen.

What are some basic steps that companies should take to protect their trade secrets?

Viscounty: Companies should create a trade secret protection program to ensure that the information they give to their employees and business partners is carefully protected. One key aspect of such a plan is ensuring that trusted employees and business partners are only given access to sensitive information when necessary. In addition, many companies only allow employees to have access to a portion of any sensitive information. For example, many companies prohibit their employees from having access to a complete client, vendor or supplier list. Instead, the relevant information should be spread among several different employees or business partners to limit the possible harm that any one person may be able to inflict.

What are some of the practices that make companies vulnerable to insider threats?

Viscounty: On a basic level, many companies have not properly identified all of their trade secrets or other confidential information, a crucial first step in any trade secret protection plan. Moreover, companies often fail to adequately inform and train the individuals and businesses that have access to their trade secrets about best practices for preventing unauthorized disclosure.

Some companies fail to audit their policies and procedures. Such audits are critical because they allow firms to evaluate whether their current trade secret protection plan is working, what changes need to be made in light of evolving business practices and whether any unauthorized disclosures have occurred. Finally, given the rapid pace of technological innovation, many companies do not adequately update and evaluate their trade secret protection plan to defend against the most current threats or make use of new security technology.

Failure to take precautions in these areas may leave a company vulnerable to hacking attacks, rogue employees or unscrupulous competitors that may target their trade secrets and, for example, sell them to foreign countries or companies, where the ability to obtain legal recourse may be limited.

What preemptive steps can companies take to defend themselves against insider threats?

Viscounty: First of all, companies must diligently vet potential employees and business partners. Proactive due diligence before a relationship begins can help avoid serious problems later on. Secondly, companies should periodically audit their security systems to search for suspicious activity and uncover areas in need of a technological upgrade. Companies must also determine whether portable storage devices, like external hard drives or thumb drives, are being used to transport sensitive information. Similarly, audits can uncover whether employees have been accessing, downloading, forwarding or printing hardcopies of sensitive information that they do not need or should not be able to access.

Uncovering these issues as early as possible can limit a company's vulnerability to trade secret theft and prevent damage from occurring in the first place.

If a company suspects an employee is mishandling or stealing information what are the first steps they need to take?

Viscounty: As a first step, the company should determine the employee's current location in case they are trying to flee the country. Indeed, the case of the former employee attempting to escape to a foreign country where legal recourse may be limited or non-existent has become a familiar and concerning pattern. If the company is able to locate the employee, the company should consider whether to contact the authorities to utilize their power to obtain a search and/or arrest warrant or apprehend the suspect and prevent them from leaving the United States with valuable trade secrets. However, before alerting the authorities, companies should be aware that they will likely lose a degree of control over the investigation, any civil actions will likely be stayed during a criminal prosecution, and the company may be forced to expend significant resources to assist in the criminal investigation.

In addition to physically stopping the employee, the company should maintain all relevant evidence with a proper chain of custody. One key piece of information is the employee's computer systems. Companies will likely want to perform a forensic investigation of the employee's computer to determine what information was downloaded, printed, copied, transferred or deleted. This investigation should also be used to update the company's trade secret program to address vulnerabilities exposed by the employee's actions. Notably, when an employee leaves a firm, many companies will give the former employee's computer to a new employee. When doing so, the company or the new employee might delete or override information from the prior user that could be relevant to a trade secret investigation or prosecution. This risk underscores the importance of preserving the chain of custody over computer systems used by employees suspected of trade secret theft.

Finally, companies should retain expert legal counsel who is familiar with international trade secret problems to make sure they are properly protecting the relevant evidence, conducting a thorough investigation, and fully informed as to whether or not to alert the authorities.

With theft of intellectual property becoming more common, is there any new legislation in the works to combat it?

Viscounty: There has been some recent legislation giving the government broader powers to protect trade secrets, particularly in cases of espionage or other threats to national security. A major focus of this effort has been an attempt to stop foreign countries from hacking into domestic computer systems or otherwise stealing sensitive intellectual property and taking it to a foreign country.

The theft of intellectual property is all too common and exceedingly expensive to American companies, so it is likely that additional legislation will be enacted to continue to help companies protect their intellectual property from theft and unauthorized disclosure.

CONTACTS

Perry J. Viscounty
Orange County, Silicon Valley
T + 1.714.755.8288
perry.viscounty@lw.com

You Might Also Be Interested In

Intellectual Property Litigation

Retail & Consumer Products

Technology Transactions

Trade Secrets Litigation