orrick

Strategic Remedies For Victims of Trade Secrets Theft

09.16.13

***Law360*, New York (September 16, 2013, 12:08 PM ET)** - Trade secret and confidential information theft by employees, perhaps in cahoots with competitors, is on the rise. Advancements in technology such as cloud computing, BYOD ("bring your own device") policies,[1] and myriad methods of information storage and retrieval have made it much more challenging for companies to impose technical barriers to prevent this type of theft. Companies are having a hard time keeping up:

- 65 percent of surveyed information and technology professionals do not know what files and data leave their firm;
- 57 percent of employees save work files to external devices every week;
- Email furnishes the quickest and easiest means for collaboration in information theft, yet is normally less protected than databases.[2]

In a recent *Law 360* article titled "You Need to Work Harder to Fight Trade Secrets Theft," authors Michael Bunis and Anna Dray-Siegel note a myriad of corporate security vulnerabilities, including the failure to secure mobile ("BYOD") devices and control access to secured networks, and recommended several strategies for reducing a company's vulnerability to the theft of intellectual property such as trade secrets. And while the strategies proposed by Bunis and Dray-Siegel should be on every company's information security checklist, a comprehensive approach to combating cybertheft includes not only making the commission of the crime more technically difficult but also disincentivizes or deters the offending conduct.

Regardless of the number of firewalls, monitoring systems and policies put in place, the world of cybertheft prevention knows no fail-safes; if an employee wants to steal information, he'll find a way. Employees must be allowed access to confidential information to do their jobs, and once they have access, misappropriation becomes possible. The key then to fighting employee cybertheft is to maximize the deterrent effect by: (1) Before the theft occurs, publish to employees the severe and immediate nature of the sanctions, and (2) once the theft occurs, make the sanction for such conduct as severe as possible.

The first step is to provide notice of potential sanctions to employees in an effort to preemptively dissuade the conduct in the first place. Employee manuals should contain clear statements describing the prohibited conduct and prescribing particular protocols for handling and safeguarding information both during and at the conclusion of employment. Because no written policy can keep up with the explosive growth of technology, the prohibited conduct should be described broadly enough to include any misappropriation. The period directly leading up to an employee departure is particularly sensitive.

Employees who will soon leave the company need a clear understanding of the requirement to return or destroy company information stored on personal laptops or PDAs. Similarly, soon-to-be-former employees must understand that access to company information stored in the cloud is strictly prohibited after their departure. And manuals should clearly notify employees that termination, civil litigation and criminal referral will all be considered by the company in the event of employee violation of these policies. In noting that criminal referral for violators is an option, the company should explain the reach of the Economic Espionage Act (18 U.S.C. § 1832) and note the associated penalties, including fines, restitution and prison time. The statutory maximum term of imprisonment for a Section 1832 violation is 10 years.

In the event of employee theft, the company must undertake a careful analysis to determine what, if any, remedy is appropriate. Assuming that the theft is well documented, the company may wish to consider termination if the culprit is still an employee. In addition, options include doing nothing, negotiating with the perpetrator, civil litigation, criminal referral or some combination thereof.

Because the federal EEA does not have a private right of action, companies wishing to file a civil lawsuit frequently must turn to the Uniform Trade Secrets Act — now law in 47 states and the District of Columbia — and sue in state court unless diversity or another basis warrants a federal action .[3] If this course is chosen, in order to establish the theft is of a "trade secret," companies must be very careful to document measures taken in the past to safeguard the information in question and must show that the relevant security measures are still in place.

Civil litigation is a particularly good option if the perpetrator is a highly solvent individual or if the perpetrator was sponsored or co-opted by a competitor company; such defendants would have sufficient assets to attach in order to satisfy a civil judgment. Also, if the company may struggle to establish the purloined material was a "trade secret," that company can bring a common law theft claim as well. Ultimately, if the goal is to deter other employees who are contemplating the same conduct, for a judgment-proof prospective defendant, civil litigation does not provide comparable deterrent value to loss of liberty.

Especially where a perpetrator is judgment-proof or difficult to reach by litigation, criminal referral may be an attractive option for corporate victims. Benefits to a corporate victim of criminal referral include enhanced deterrence (loss of liberty is a great deal more serious than loss of money, especially to the judgment-proof), restitution of the value of the trade secrets, leverage over the perpetrator to incentivize him to share what he did with the ill-gotten

information, and the potential for recovering fees associated with the investigation undertaken by the company in the course of the referral, a remedy not normally available in the course of civil litigation.

The trail for fee recovery was blazed in part in February 2013, when former Goldman Sachs Group Inc. director Rajat K. Gupta was ordered to reimburse Goldman Sachs $6.2 million for legal fees that the company incurred in the course of its internal investigation of Gupta's trading practices. Access to such restitution under the Mandatory Victim Restitution Act is limited to crime victims who have incurred losses as the result of a criminal defendant's wrongful conduct, and the act's provisions are mandatory.

Companies must demonstrate that the fees requested were "necessary" and "incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense" by a "victim." (Note that some courts have declined to apply the MVRA's language to a voluntary internal investigation undertaken well before any criminal prosecution; for these courts, the investigation must be either required or requested by government investigators or prosecutors.)

If referral is made to a federal prosecutor the two statutes most often in play are the Computer Fraud and Abuse Act (18 U.S.C. § 1030), which criminalizes accessing a computer without authorization or exceeding authorization, and the EEA, which prohibits the theft of trade secrets. Prosecution under the CFAA provides an important backstop where theft of the purloined material may not amount to a violation of the EEA. This could be because the material may not meet the definition of a "trade secret" or insufficient protective steps may have been taken to safeguard it.

Further, if the material is not a trade secret, there is no federal theft of confidential information not amounting to a trade secret. To mitigate against the risk that a court may find the material was not a trade secret, a federal prosecutor will want an additional crime upon which to gain conviction. Hence, a violation of the CFAA. The CFAA criminalizes conduct by an employee that constitutes computer hacking but, depending on which region of the country you are in (there is a circuit court split on the issue), also punishes an employee accessing corporate computer-based information that he or she was not authorized to access.

Civil litigation and criminal referral are premised on the victim company undertaking a careful and thorough internal investigation. It is critically important to avoid the appearance of collusion with the perpetrator and, whichever course is followed, to provide the court or the prosecutor with a complete and well-structured package of information regarding the theft. And, in the first instance, in order to understand what course, if any, it should take in responding, the victim company needs to know exactly what happened, including what the employee did with the purloined information. It's especially important to know whether the information has gone to a new employer or competitor who is now using it in an anti-competitive way. To this end, the investigation should be conducted by an attorney, who can maintain the confidentiality of the information under the attorney-client privilege while hiring forensic investigators to do the investigatory work.

In considering whether criminal referral is appropriate, the attorney advising a victim company must tread very carefully. Despite the advantages in restitution described above, criminal referral has its own potential trapdoors; inviting the government into your life comes with a price tag.

First, once the matter has been referred, the referral cannot be withdrawn — the victim company loses control over it. Second, depending on the prior actions and policies of the company, it may face some amount of adverse publicity or even liability. Third, and relatedly, the company itself may have areas of vulnerability that make government involvement disadvantageous or even dangerous to the company's reputation. Finally, criminal referral potentially brings with it the significant cost of responding to government subpoenas and making employees available to testify. Victim companies should carefully consider whether they are willing to spend the associated time and money.

If the victim company decides to make the criminal referral, there remains significant uncertainty as to whether the government will take the case. The government tends to be most interested in cases involving thefts of extremely valuable trade secrets or trade secrets that have been used in an anti-competitive way. Here, a victim company will increase its chances of success if it:

- conducts and packages a thorough investigation that reduces the amount of work required to prosecute the case;
- determines the sovereign: federal, state or local, the law enforcement agency and the venue that will be most hospitable to the matter; and
- locates a prosecutor who will be interested in taking the case.

The example of David Nosal is instructive. Nosal left Korn/Ferry International to start a competing executive search firm and was suspected of colluding with then-current Korn/Ferry employees to steal his former employer's trade secrets. After it discovered Nosal's conduct, Korn/Ferry made the criminal referral and filed a civil suit as well. And while the civil lawsuit was transferred to a confidential arbitration setting, on April 25, 2013, Nosal was publicly convicted of violating the CFAA and the EAA. His Oct. 9, 2013, sentencing, where he is facing a multiple-year prison, is sure to send a strong message of deterrence to fellow Korn/Ferry employees contemplating the same behavior.

Theft prevention is always the gold standard. But potential sanctions, including criminal referral, add bite to prevention strategies so that employees think twice or even longer before engaging in conduct that is unfortunately becoming more and more commonplace.

--By **Mark Mermelstein** and **Mary Kelly Persyn**, Orrick Herrington & Sutcliffe LLP

Mark Mermelstein is a partner in Orrick's corporate crimes and investigations group in Los Angeles. Mary Kelly Persyn is a managing associate in the firm's corporate crimes and investigations and appellate groups in San Francisco.

[1] The number of devices that can connect to the Internet and other networks is expected to increase from about 12.5 billion in 2010 to 25 billion in 2015, increasing by orders of magnitude the ability of malicious actors to exploit security vulnerabilities and steal information. Office of the National Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage ("ONCE Report"), 2009-2011 (October 2011), at 6.

[2] ONCE Report at A-3.

[3] Congress is considering adding a private right of action to the Economic Espionage Act by means of the Protecting American Trade Secrets and Innovation Act of 2012. If passed, the law will allow an additional range of remedies, including empowering federal courts to issue ex parte seizure orders.

Authors

Mark Mermelstein
Partner, White Collar, Investigations, Securities Litigation & Compliance, Internal Investigations

Los Angeles

D +1 213 612 2204
E mmermelstein@orrick.com