An ALM Publication

CORPORATE COUNSEL

LEGAL MANAGER
06 | 2011

A GOOD DEFENSE

Some tips on fighting back against industrial espionage.

[BY CARLOS PEREZ-ALBUERNE]

DISCUSSION OF INDUSTRIAL ESPIONAGE, much like press accounts of state-sponsored spying, conjures up images of unknown shadowy figures using sophisticated surveillance techniques and advanced software to gain access to their competitors' secrets.

While there have indeed been instances in which corporate thieves have employed cutting-edge technology to procure secrets, reported cases of this kind are relatively rare. Much more common are less dramatic uses of old-school techniques by which someone legitimately gains access to a company's sensitive information but then betrays that trust. Here are some common ways that industrial espionage occurs, and some tips on ways to combat both the older and newer versions of it.

Defectors have always been a key resource for competitors seeking to obtain information the easy way. A competitor recruits a key employee and gets him to spill the beans on his old company's plans and emerging technologies. The former employee also brings along with him and shares copies of recent business plans and any "secret sauce" intellectual property schematics he can get his hands on.

This mode of industrial espionage is still the most common danger to a company's trade secrets. But with some relatively simple processes, this risk can be significantly mitigated.

First, companies should ensure that their key employees' noncompete and confidentiality agreements are comprehensive and up-to-date.

Second, companies should develop a "key departure" checklist that their HR departments and management can use to ensure that the company's intellectual property is safeguarded when a key employee leaves. For example, IT departments can conduct a review of that employee's computer activities in the weeks prior to his departure. In particular, they can see if the employee (1) downloaded key documents to a portable storage device; (2) forwarded documents to a personal e-mail address; or (3) printed an unusually large volume of documents. Company-owned computers and storage devices should also be inventoried and collected. The departing employee should be reminded of his ongoing confidentiality obligations. He should also be required to represent that he understands those obligations and that he is not taking any such information with him (apart from whatever resides between his ears).

If these measures are not in place (or prove inadequate) and a company believes that its former employee has stolen company secrets, it is crucial that it devise a legal strategy that focuses, at least in part, on immediately obtaining key evidence before the adversary can destroy it. For example, courts may be willing under certain circumstances to order ex parte relief that compels the immediate creation of forensic images of the former employee's laptop and personal e-mail account. Obviously, you cannot rely on a potential defendant's good faith to preserve evidence in circumstances like this where those parties have already stolen a company's intellectual property and given it to competitors.

In particular circumstances, companies may also consider requesting that a U.S. attorney's office become involved, as the government has enhanced techniques for preventing the destruction of evidence and for further deterring the transmittal of trade secrets. Additionally, aggrieved companies have increasingly sought relief in federal court under the Computer Fraud and Abuse Act, although there is currently some disagreement among federal appellate courts concerning the breadth of civil remedies under this statute.

Use of a "mole" remains one of the most common ways to gain unauthorized access to your information. A competitor recruits a company's current employee to provide it with sensitive information. While this technique is decidedly old-school, it may be the most devastating. Unlike pumping a defecting employee for information, corrupting a current employee can provide an ongoing stream of trade secrets. A competitor can target a current employee to collect information to satisfy an evolving set of needs.

There are a few ways to mitigate this risk. First, companies can ensure that they share their critical trade secrets with only those employees who need to know the information. While this defensive strategy sounds obvious, it is surprising how few companies focus on the following ways to actually execute this strategy: (1) identify exactly what information should be protected as company

secrets; (2) develop a plan to limit access to that information; and (3) assign someone (or a team) with responsibility to police access and maintain accountability.

Second, IT departments should periodically conduct audits to ensure that network access to critical documents is reasonably restricted. Third, companies must be cautious about entrusting their company's most sensitive information to employees whom they just hired away from their chief rival. Some recent cases have involved a company sending a trusted employee to work for their competitor with the understanding that the employee would secretly provide information to their old company, to whom they would eventually return, greatly appreciated.

AND THEN THERE ARE VARIOUS TYPES of outsiders to worry about. Some companies, while desperately wanting access to their competitors' plans, do not wish to bear the risk of obtaining that information through improper means. This creates a market for intermediaries who can steal the information and then provide it to customers without telling them how they obtained it. Many customers will pay a significant premium for increased knowledge of their competitors' plans, along with plausible deniability about how that information came to their desks. They simply farm out the dirty work to unscrupulous operatives who are willing to steal proprietary information for cash.

There are two varieties of such "Trojan horses," the high-tech and the low-tech. Let's consider the high-tech variety first. A company provides a consultant with brief access to its computer networks to conduct a project. While on the network, the consultant uploads a Trojan horse computer program. The Trojan horse malware (malicious software) contains code that provides the consultant with the ability—after his project has been completed—to remotely and secretly regain entry to the network, where he has access to the entirety of the company's records and e-mails.

In situations where consultants are going to work within your company's IT infrastructure, your consulting agreements should include provisions that require disclosure of appropriate background information about the actual people working on the project and for this disclosure to be made sufficiently in advance that it can be reviewed and potential problems can be addressed. For example, many consultants use freelance talent themselves—and some of that is located offshore. Those individuals may have little incentive to comply with confidentiality obligations—due to both the mercenary nature of their employment and the difficulties in pursuing them abroad. Depending on the scope of the project, IT security issues like these should be made part of the request for proposals process.

Companies can lose sight of how far they may be SPREADING THEIR CONFIDENTIAL INFORMATION in the rush to get a deal done.

Then there's the low-tech version of the Trojan horse operative. A company seeks to sell some of its technology assets and provides a competitor with due diligence access to that technology. Instead of buying the assets, the competitor takes the know-how back to a distant jurisdiction and uses it to create a new product. It is easy for companies to lose sight of just how far they may be spreading their confidential information in the rush to get a deal done.

But before providing a competitor with access to sensitive technology, a company should ask the competitor some questions to evaluate whether they are actually serious in pursuing the assets. Companies should also stage the diligence process carefully so that sensitive information is not disclosed until as late in the negotiations as possible. Also, while a nondisclosure agreement that expressly calls for preliminary injunctive relief is nice, a company should evaluate its enforceability in the competitor's location, particularly if the competitor is based in or has operations in a foreign country that lacks appropriate protection for intellectual property.

Finally, there are the really low-tech operatives, the old-fashioned dumpster divers. A competitor literally has people dig through a company's trash for documents that describe business plans, intellectual property, and other trade secrets. This technique is low-cost as well as low-tech. Luckily, it is also pretty easy to combat, including by firming up internal procedures, by expanding access to shred bins, and by conducting random inspections of discarded materials.

While the vast majority of market research, competitive intelligence, and expert firms operate well within ethical and legal boundaries, inevitably some do not. Companies should advise their employees with access to sensitive information to be alert to contacts from outside firms regarding their work and to report any unusual overtures. When it comes to breaches of your proprietary information, you can greatly limit the chances of exposure by implementing the measures described above.

Carlos Perez-Albuerne is a partner in the Intellectual Property Litigation Group at Choate, Hall & Stewart in Boston. He can be reached at cperez@choate.com.