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

Does Your Company Need An IP Protection Audit?

Law360, New York (June 14, 2011) -- The answer, like many things, is “it depends.” But you do need to understand the question and the potential value of undertaking such an audit.

Litigation flowing from the failure to protect new or developing confidential information, and particularly international trade-secret theft, is on the rise. Barely a week passes now without a major lawsuit or legal development in this area, often with tens of millions of dollars at stake. Confidential information such as products in development, client lists, and pricing and cost data are at the heart of most companies. The business and legal strategies for protecting them require thoughtful analysis and action at the front end, before your company is the victim.

Recently, a California jury awarded a major health care company a $2.3 billion verdict against a former employee and the Chinese medical device company he started on claims of trade secret misappropriation. A company spokesperson heralded “the message” the verdict sends to would-be intellectual property thieves. Messages are important, but one has to wonder if the verdict is really a win. After the trial, Law360 reported, the jury foreperson astutely told to the victorious lawyers, “Good luck collecting.”

And therein is the crux of the problem: Once the information is out, you cannot “unring the bell” in the Internet age, and shutting down the offenders and collecting damages may not be possible. Getting jurisdiction over foreign actors may be challenging, particularly if the theft and misuse occurred outside the U.S. Furthermore, some other countries do not recognize theft of intangible property as a legally cognizable claim. Even if a case can be made, as in the case of the heath care company, the thieves may not be in a position to fully compensate the company for the damages done.

Your first line of defense is usually the IT department and the security in your physical spaces. In this regard, a one-size-fits-all approach cannot work. The appropriate level of protection is a matter of balancing the need to maintain confidentiality for certain highly valuable information — such as data related to products in development — without squelching efficiency and innovation. Also, information security can be expensive. So there is a need to apply it in a targeted fashion.

On the legal side, the place to start is often with employment agreements. This usually requires an interdisciplinary approach involving both the IP lawyers and labor and employment lawyers, which can be challenging in a large legal department or across different parts of the company.

Nondisclosure clauses and the like are the easy part. You should ask the harder questions, like: “What recourse will I have against a departed employee or contractor? What will incentivize him to keep my information secret?” Here, the human resources and benefits departments within your company may be involved. Again, a one-size-fits-all approach here may not make sense. Target your efforts to employees who are in positions to receive information that must be protected.

The next step is to prepare for litigation before it happens. Trade secret misappropriation cases often turn on the extent to which the information is actually kept secret. So monitor the program. Consider having someone in the legal department educate the new product development teams on appropriate practices for data management. You may also want to periodically check in to see if adjustments to the governing protocols are necessary.

Finally, try to identify risks and manage them effectively. Once your employee is overseas using your confidential information with another company, your options are limited. Effective off-boarding procedures, including the use of forensics, to identify risks are necessary. Tracking former employees and monitoring the market place generally can also be helpful. Again, the more customized the programs, the better.

Once risks are identified, you can develop a strategy with your counsel. If litigation is necessary, it is usually wise to initiate right away. Thus, having outside counsel who are already familiar with your protocols and can act quickly to protect your rights is very often critical to success. Indeed, this may be the most important reason to undertake an IP protection audit.

--By Mark Klapow, Crowell & Moring LLP

Mark Klapow is a partner in the litigation group of Crowell & Moring in the firm's Washington, D.C., office.