DECEMBER 12, 2015 FORTUNE

Cyber Espionage Is Reaching Crisis Levels

The digital age is plaguing companies with new threats from abroad.

By Pamela Passman
CEO
CREATe.org

By David J. Kappos
Corporate Partner
Cravath, Swaine & Moore LLP

It's no secret that companies work hard to protect their intellectual property from theft. For innovations where confidentiality is integral to value, trade secrecy law offers a bargain: make reasonable efforts to maintain confidentiality, and those efforts will be backed up by legal sanctions. However, the rise of cybercrime is forcing companies to reevaluate the way they protect their most valuable trade secrets.

Trade secret theft costs companies billions of dollars every year. Traditionally, these crimes took the form of bribing, dumpster-diving or, as in one famous case, aerial photography. These days, industrial espionage has gone digital, introducing new threats and magnifying the impact of established techniques. Even employee raiding, an age-old tactic of trade secret mis-appropriators, is made more problematic in modern times by the sheer volume of secrets that can be stolen via digital media.

But a still more ominous threat spawned by the digital age comes from remotely launched computer attacks. Cyber espionage has reached crisis levels. One study puts the cost of cybercrime at $24 billion to $120 billion in the U.S. and up to $1 trillion globally.

For modern corporations, the cross-border aspects of cyber espionage can cause significant challenges. One stark example of the difficulty of prosecuting international cyber espionage is the plight of AMSC, a U.S. firm specializing in software for wind turbines whose core product was allegedly stolen by Chinese turbine manufacturer Sinovel Wind Group Co. in 2011. Sinovel reportedly convinced an AMSC engineer to misappropriate code from Wisconsin, decrypt it in Austria, and email it to China. AMSC did not promptly detect the IT breach; rather, it identified the leak only after accidentally discovering its code in a Sinovel test facility in China.

By the time AMSC launched a cyber investigation, contacted the FBI, and ultimately obtained an indictment, counterfeit copies of their software had already been sold back into the United States in Sinovel's products. Hamstrung by deficient cyber-intelligence, AMSC's legal action proved to be too little too late. The named defendants are now all in non-extradition countries and Sinovel has deployed litigation defense tactics that have stalled the case in U.S. courts while AMSC's stock has fallen from $370 per share to $5 per share.

The executive and legislative branches of the U.S. Government have ramped up anti-cyber espionage efforts and are on course to amend the Economic Espionage Act of 1996 to create a federal civil remedy for trade secret theft. These efforts, coupled with increased enforcement of trade secret laws at the state level, will address the majority of misappropriation that occurs domestically.

However, acts of trade secret theft originating from outside the U.S. continue to be difficult to address. In recent times, both domestic and international companies have begun to bring cases before the U.S. International Trade Commission (ITC). In 2011, the Federal Circuit concluded that the ITC "has authority to investigate and grant relief based in part on extraterritorial conduct insofar as it is necessary to protect domestic industries from injuries arising out of unfair competition in the domestic marketplace."

This has been a helpful development, as the ITC is able to provide U.S. companies with a potent avenue of redress. It has the power to issue broad exclusion orders blocking importation and to draw adverse inferences against foreign parties who are non-responsive. Though the ITC cannot directly police the business practices of companies overseas, its adjudications can severely curtail the thieves' advantages.

All this firepower needs to be backed up by robust trade secret identification and protection programs, along with vigorous misappropriation detection and response capabilities. These moves are critical to building the "evidence" that U.S. corporations need to successfully bring and win legal actions against cyber-facilitated trade secret theft, no matter its origin.

The implementation of an effective trade secret program is no longer within the skill set of any one department. Rather, cyber defense now requires a cross-functional dynamism between legal departments and internal cybersecurity information technology teams. These proactive joint efforts must align to identify and safeguard trade secrets before cyber thefts are carried out, and to respond when attacks do occur, in order to capture, isolate, retain and use the "evidence" needed to bring — and win — cases against cyber perpetrators.

By addressing trade secret protection in the broader context of "people, processes and technology," companies can ensure that they are mitigating risks, more quickly identifying breaches and ultimately securing the information required to take meaningful action. This line of attack requires breaking down silos within companies and building strong, structured pathways for collaboration between cybersecurity and legal experts. This may require a realignment of organizational capabilities, but such a move is critical to enforcement and will ultimately deter cyber thieves, both domestic and foreign. At a projected annual savings in the many billions of dollars, innovative companies can hardly afford not to invest in this collaboration.

David J. Kappos is a partner at New York City-based law firm, Cravath, Swaine & Moore LLP, where he supports the firm's clients with a wide range of intellectual property issues. From August 2009 to January 2013, Kappos served as director of the U.S. Patent and Trademark Office. He is a senior advisor for the Partnership for American Innovation. Pamela Passman is CEO of the Center for Responsible Enterprise and Trade (CREATe.org), an NGO that helps companies and their third parties prevent corruption and protect intellectual property and trade secrets. Prior to founding CREATe, she was CVP and Deputy General Counsel at Microsoft Corporation.