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

Keeping Secrets Secret: A Primer On Economic Espionage


Joseph Walker

Law360, New York (September 03, 2013, 11:49 AM ET) -- The theft of corporate trade secrets and other intellectual property is a growing concern both for victims of theft and those accused of such misappropriation. This article aims to examine both sides of the coin, and proffers guidance for companies who seek to protect their proprietary information from economic and industrial espionage as well as ensure that they themselves are not accused of any wrongdoing.

The Commission on the Theft of American Intellectual Property estimates that annual losses of international intellectual property theft affect the U.S. economy to the tune of over $300 billion.[1] This number does not include the job losses associated with such theft as well as the diminished incentive to innovate.[2] Businesses frequently targeted by economic espionage include "high tech businesses, pharmaceutical companies, manufacturing firms, and service industries."[3]

Industries that are frequently targeted include "aerospace, biotechnology, computer software and hardware, transportation and engine technology, defense technology, telecommunications, energy research, advanced materials and coatings, stealth technologies, lasers, manufacturing processes, and semiconductors."[4]

Recent examples of trade secrets that have been allegedly misappropriated include: cellular glass insulation used in buildings, industrial piping systems, and liquefied natural gas storage tank bases[5]; fiber used, inter alia, in body armor, fiberoptic cables, and automotive and industrial products[6]; a silicon gyroscope designed for use in micro-navigator systems, target locators, munitions, and other military applications[7]; a computer code for an electronic trading platform[8]; telephone communications technology[9]; customer and pricing information of sprinkler and irrigation products[10]; chloride-route titanium dioxide[11]; chemical compounds developed for pharmaceutical and healthcare applications[12]; and chlorinated polyethylene.[13]

Companies face threats not only from individuals or companies who seek to gain for their own personal benefit, but also from foreign governments: A study released in early 2013 indicated that China's People Liberation Army may have been responsible for attacks against American corporate networks in which intellectual property was stolen.[14]

The Federal Bureau of Investigation has noted that foreign competitors who seek proprietary information generally operate in three ways: aggressively targeting and recruiting insiders, conducting economic intelligence (e.g., cyber intrusions), and establishing "seemingly innocent business

relationships between foreign companies and U.S. industries to gather economic intelligence."[15] The FBI recommends that companies take the following steps to protect themselves from espionage: (1) recognize potential insider and outsider threats, (2) identify trade secret information, (3) implement plans for safeguarding trade secret information, (4) secure physical and electronic versions of trade secrets, (5) limit intellectual knowledge on a "need-to-know" basis, and (6) provide training to employees about the company's intellectual property plan and security.[16]

The Economic Espionage Act (as well as most civil remedies available via state law) requires that a trade secret owner take "reasonable measures" to keep information secret. 18 U.S.C. § 1839(3)(A). Reasonable measures that a company can take to protect its confidential proprietary information include executing agreements with its employees that require them not to disclose secret or confidential information, either during or after their period of employment, absent prior written consent; conducting exit interviews; requiring employees to pledge that upon termination they will promptly return all material of a secret or confidential nature; having security guards check employees' identification before entering a building or secure area; reserving the right to search employees' belongings and cars; holding training sessions to instruct employees not to share information with outside parties; and marking proprietary documents accordingly.[17] Computer or electronic protections (e.g., passwords, data encryption, and limiting remote or internet access in areas where trade secrets are used or located) are also examples of reasonable measures.[18]

The U.S. government is also taking steps to protect confidential information belonging to U.S. companies. Currently pending in the Senate is the Deter Cyber Theft Act.[19] The act would require the director of national intelligence ("DNI") to develop a watch list of foreign countries that engage in economic or industrial espionage. It would also require the president to block imports of products (1) containing stolen U.S. technology or proprietary information, or (2) that are produced by a state-owned enterprise of a country on the priority watch list and that are the same as or similar to products made using stolen or targeted U.S. technology or proprietary information identified in the report from the DNI, or (3) that are made by a company identified in the DNI report as having benefited from the stolen U.S. technology or proprietary information.[20]

China is the country that probably poses the greatest threat to the theft of American proprietary information right now. The Commission on the Theft of American Intellectual Property, noting that while the "major studies range in their estimates of China's share of international IP theft," many of the studies estimate that China contributes to roughly 70 percent of international theft.[21] Government offices and agencies are also actively seeking to curb theft of American intellectual property by other countries and foreign entities. For example, the U.S. Patent and Trademark Office offers training and education programs in the United States and abroad about protecting and enforcing intellectual property rights, and the U.S. Department of State offers similar programs as well through its International Visitors Leadership Program.[22]

Avoiding Accusations of Economic Espionage or Theft of Trade Secrets

Allegations of misappropriation of trade secrets or other intellectual property expose companies and individuals to serious criminal and civil liability. It is not uncommon for civil lawsuits to ripen into criminal indictments.[23] The Economic Espionage Act prohibits both economic espionage (i.e., theft of trade secrets for the benefit of a foreign government)[24] as well as theft of trade secrets (i.e., theft of a trade secret for a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof).[25]

Those found guilty of the latter offense may be fined or imprisoned for up to 10 years, or both.[26] Organizations that commit theft of trade secrets may be fined up to $5 million.[27] Individuals found guilty of economic espionage face a fine of up to $5 million and imprisonment of 15 years;[28] organizations found guilty of economic espionage will be fined not more than the greater of $10 million or three times the value of the stolen trade secret to the organization.[29]

Besides prosecution for economic espionage and/or theft of trade secret under the Economic Espionage Act, other related charges could include: unauthorized disclosure of government information; violations of the Arms Export Control Act and International Traffic in Arms Regulations; computer fraud; unauthorized access via a computer; intrusion; mail/wire fraud; transportation of stolen property; money laundering; false statement; obstruction of justice; and forfeiture.[30]

Conviction is also possible under 18 U.S.C. § 951, which prohibits persons from acting as unregistered foreign agents.[31] For sentencing purposes following conviction, the U.S. Department of Justice has identified the following as appropriate measures of the loss suffered by the victim: (1) research and development costs; (2) the amount for which the defendant sold the information; (3) the amount for which similar information has been sold in the open market; (4) licensing or royalty fees for the information; (5) the "fair market value of the business or product line that could be infringed upon by a competitor with access to the trade secret"; and (6) "any other methodology that calculates the reasonable foreseeable pecuniary losses caused by the defendant's conduct."[32]

When determining whether to prosecute under the Economic Espionage Act, a United States Attorney's Office considers the following: "(a) the scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality; (b) the degree of economic injury to the trade secret owner; (c) the type of trade secret misappropriated; (d) the effectiveness of available civil remedies; and (e) the potential deterrent value of the prosecution."[33] Whether a civil remedy is available is not a dispositive factor since "the victim of a trade secret theft almost always has recourse to a civil action."[34]

There are several actions a company can take to avoid being prosecuted, let alone sentenced, for violations of the Economic Espionage Act. For example, a company should request information from new hires about any noncompetes and/or confidentiality agreements, and should have a clear policy in place that alerts all employees that the company does not engage in or approve of any sort of misappropriation.

Moreover, a company should promptly investigate and/or report any suspicious behavior by employees or outside parties.[35] Even though compliance takes time and costs money, expenditure of these resources is less expensive in the long run than leaving deficient safeguards in place that fail to identify employees who may be engaging in economic espionage that can expose the company to serious risks and costs.

--By Joseph Walker and Rebecca Worthington, Squire Sanders LLP

Joseph Walker is a partner and Rebecca Worthington is an associate in Squire Sanders' Washington, D.C., office.

clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Comm'n on the Theft of Am. Intellectual Prop., IP Commission Report, May 2013 at 2, available athttp://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

[2] Comm'n on the Theft of Am. Intellectual Prop., IP Commission Report, May 2013 at 2, available athttp://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

[3] Hedieh Nasheri, Economic Espionage and Industrial Spying, 9 (Cambridge University Press 2005).

[4] Hedieh Nasheri, Economic Espionage and Industrial Spying, 9 (Cambridge University Press 2005).

[5] See United States v. Huang, Case No. 4:12-cr-296, Western District of Missouri. Defendants met with an employee of Pittsburgh Corning to arrange for the employee to provide copies of documents contacting trade secrets related to the formula and manufacturing process for the insulation.

[6] See United States v. Kolon Indus., Inc., Case No. 3:12-cr-137, Eastern District of Virginia. Defendant allegedly sought to obtain the trade secrets by hiring and attempting to hire former and current employees of DuPont and other companies as consultants. Defendant then asked these "consultants" to reveal confidential, proprietary information, particularly regarding the manufacturing process.

[7] See United States v. Liu, Case. No. 2:11-cr-208, District of New Jersey. Defendant had in his possession a white paper containing scientific, technical, and engineering information related to the gyroscope. The gyroscope was developed for intended sales to defense contractors for integration into military devices.

[8] See United States v. Yang, Case No. 1:11-cr-458, Northern District of Illinois. Defendant was an employee of the victim (a trading exchange company), and downloaded thousands of files containing the computer source code from a secure internal computer to his work computer. He then transferred files from his work computer to personal computers via a personal USB flash drive.

[9] See United States v. Jin, Case. No. 1:08-cr-192, Northern District of Illinois. Defendant was employed by the victim company as a software engineer. She downloaded numerous technical documents belonging to the company off the company's secure internal computer network. She was charged both with theft of trade secrets and economic espionage, as she allegedly stole trade secrets to benefit the military of the People's Republic of China.

[10] See United States v. Capener, Case No. 1:12-cr-27, District of Utah. One of the defendants worked in one of the victim company's factories in Ningbo, Zhejiang Province, China. On the day she was informed her employment would be terminated, the defendant allegedly accessed the company's intranet and downloaded substantial amounts of sales and pricing information.

[11] See United States v. Liew, Case No. 3:11-cr-573, Northern District of California. According to the Superseding Indictment, the government of the People's Republic of China publicly identified the development of this technology as a "scientific and economic priority." The defendants allegedly obtained trade secrets belonging to the victim company (DuPont) and gave this information to companies controlled by the PRC government. Defendants allegedly obtained confidential information about DuPont's plant costs and personnel data, as well as photographs from various DuPont facilities

containing proprietary, confidential information about DuPont's technologies associated with the chloride-route titanium dioxide process.

[12] See United States v. Li, Case No. 3:12-cr-34, District of New Jersey. Defendant was a Chinese national and employed by the victim company (Sanofi) as a medicinal chemist. Defendant was a 50% partner in Abby Pharmatech, Inc., which purported to be a United States subsidiary of a Chinese-based chemical production company. Defendant accessed a Sanofi internal database and downloaded information related to certain compounds, including their chemical structure. She then transferred the downloaded information to a personal computer, assigned Abby Pharmatech numbers to the chemical structures of the Sanofi Compounds, and advertised them for sale in the Abby Pharmatech catalog and website.

[13] See United States v. Liu, Case No. 3:05-cr-85, Middle District of Louisiana. Chlorinated polyethylene polymer has a wide range of uses, including but not limited to automotive and industrial hoses, electrical cable jackets, vinyl siding, and window profiles. Defendant worked for the victim company (Dow Chemical Company) in research and development. He allegedly possessed certain materials related to the trade secret, including process index flow sheets, process flow diagrams, piping and instrumentation diagrams, engineering drawings, the Dow process manual, and correspondence.

[14] David M. Ewalt, Chinese Army Directing Cyber Espionage Against Western Businesses, Forbes, Feb. 19, 2013, available athttp://www.forbes.com/sites/davidewalt/2013/02/19/chinese-army-directing-cyber-espionage-against-western-businesses/.

[15] Economic Espionage, http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage.

[16] Economic Espionage, http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage.

[17] See United States v. Kolon, (Case No. 3:12-137, E.D. Va.), Aug. 21, 2012 Indictment at paragraphs 25, 27; United States v. Chung, 659 F.3d 815, 827 (9th Cir. 2011) (finding there was sufficient evidence to support the conclusion that the victim took reasonable measures to keep certain documents secret).

[18] Mark L. Krotoski, Economic Espionage and Trade Secrets: Common Issues in Prosecuting Trade Secret and Economic Espionage Cases, in 57 United States Attorneys' Bulletin, 10 (Nov. 2009).

[19] S.884, 113th Cong.

[20] 159 Cong. Rec. S3161, S3166 (daily ed. May 7, 2013) (statement of Sen. Levin).

[21] Comm'n on the Theft of Am. Intellectual Prop., IP Commission Report, May 2013 at 3, available athttp://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

[22] Office of the U.S. Trade Representative, 2013 Special 301 Report, May 2013 at 16-18, available at http://www.ustr.gov/about-us/press-office/reports-and-publications/2013/2013-special-301-report.

[23] For example, in September 2011 the jury in E.I. Dupont De Demours & Co. v. Kolon Indus., Civil Action No. 3:09-cv-58, (E.D. Va.), found that the defendant violated the Virginia Uniform Trade Secrets Act when it willfully and maliciously misappropriated and used the plaintiff's trade secrets by, inter alia,

retaining as consultants former DuPont employees whom it paid to divulge DuPont's trade secrets. In 2012, Kolon Industries, along with several individuals, were indicted in the Eastern District of Virginia (Case No. 3:12-137) for conspiracy to convert trade secrets, theft of trade secrets, and obstruction of justice. The indictment revolved around DuPont's trade secrets that were the subject of the civil lawsuit. Another example is United States v. Liu, Case No. 3:05-cr-85, Middle District of Louisiana. Prior to the criminal action, a civil suit was filed in the Middle District of Louisiana by the victim company against Defendant Liu. See Dow Chemical Company and DuPont Dow Elastomers, LLC, v. Wen-Chyu, Civil Action No. 99-544-C-M3.

[24] See 18 U.S.C. § 1831.

[25] See 18 U.S.C. § 1832.

[26] 18 U.S.C. § 1832(a).

[27] 18 U.S.C. § 1832(b).

[28] 18 U.S.C. § 1831(a).

[29] 18 U.S.C. § 1831(b). This includes the "expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided." Id.

[30] Mark L. Krotoski, Economic Espionage and Trade Secrets: Common Issues in Prosecuting Trade Secret and Economic Espionage Cases, in 57 United States Attorneys' Bulletin, 21-22 (Nov. 2009).

[31] See, e.g., United States v. Chung, 659 F.3d 815, 823-24 (9th Cir. 2011). Besides being convicted of six counts of violating the Economic Espionage Act, the defendant was also convicted of acting as an unregistered foreign agent when he acted under the direction or control of Chinese officials (e.g., gathering and delivering "technical information regarding the structural design of aircraft in specific response to requests from Chinese officials").

[32] Christopher S. Merriam, Economic Espionage and Trade Secrets: Addressing Sentencing Issues in Trade Secret and Economic Espionage Cases, in 57 United States Attorneys' Bulletin, 64-67 (Nov. 2009).

[33] USAM § 9-59.100.

[34] USAM § 9-59.100.

[35] See, e.g., United States v. Williams, 526 F.3d 1312, 1316-17 (11th Cir. 2008). Pepsi received a letter from someone alleging to be a high-level employee for Coca-Cola, claiming that they had detailed and confidential information about Coca-Cola's marketing campaign. Pepsi then faxed a copy of the letter to Coca-Cola, who in turn contacted the FBI.
