Published on *The National Law Review* https://natlawreview.com

Series: Types of Industrial Espionage

Article By:

Benjamin C. Glassman

Colin R. Jennings

Woli I. Urbe

Industrial espionage refers to various activities performed to gain an unfair competitive advantage, rather than for national security purposes. As we discussed in a previous article, the ways in which industrial espionage can affect a company are numerous and include theft of trade secrets and disruption to operation.

Section 1832 of the Economic Espionage Act of 1996 (the "Act") criminalizes the theft of trade secrets "intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner." The trade secret owner is required to take "reasonable measures" to keep the information secret. For individuals, convictions in violation of 18 U.S.C. § 1832 can result in a prison sentence of up to 10 years or a monetary penalty, or both. For organizations, the fine may be "not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret . . . including expenses for research and design and other costs of reproducing the trade secret." Section 1832 requires that the products be "produced for" or "placed in" interstate or foreign commerce.

Before the passage of the Defend Trade Secrets Act of 2016 ("DTSA"), which amends the Act to include a federal civil cause of action for the misappropriation of trade secrets, companies relied on state civil laws for the misappropriation of trade secrets, or an independent federal cause of action to seek redress for the misappropriation of trade secrets. Currently, 48 states and the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted some form of the Uniform Trade Secrets Act ("UTSA"). New York and North Carolina are the only states that have not enacted some form of the UTSA. The DTSA does not preempt existing state trade secrets laws, but provides companies another option for filing suits in federal court. A further discussion of the available remedies to affected entities will be examined in a subsequent blog post.

Cyberattacks

While cyberattacks (e.g. malware, ransomware, and denial of service attacks) can be used to collect confidential company information, they can also be used to disrupt a company's computer system(s) for commercial gain.

In 2017, River City Media, LLC, a Wyoming corporation that engages in internet-based marketing, alleged, among other things, that Kromtech Alliance Corporation, CXO Media Inc., International Data Group Inc., and related individuals, systematically infiltrated their data network, illegally gained access to their databases without authorization, and then copied, modified, and damaged its confidential, sensitive, and propriety information, in violation of Section 1832 of the Act. River City Media, LLC. v. Kromtech All. Corp., No. 2:17-cv-00105-SAB, 2017 U.S. Dist. LEXIS 137938 (E.D. Wash. Aug. 28, 2017).

River City alleged that a then-unknown threat actor connected to one of its servers that was used to monitor River City's network for potential intruders. The threat actor destroyed data that mapped River City's network, thereby hamstringing River City's ability to detect and stop additional cyberattacks. Further, the threat actor accessed River City's: (1) company email accounts; (2) Dropbox.com account; (3) accounts for affiliate networks; (4) PayPal accounts; and (5) its email service provider accounts. River City alleged that the defendants used the data obtained by the cyberattack to attack and damage River City's reputation via media and blog postings. The parties settled the dispute prior to trial.

Disgruntled Employee

An outgoing employee can download or copy proprietary information and sell that information to a competitor or engage in unfair competition. In United States v. Lange, Matthew Lange was sentenced to thirty months in prison for violating Section 1832 of the Act. 312 F.3d 263 (7th Cir. 2002). Lange was a former employee of Replacement Aircraft Parts Co. ("RAPCO") accused of stealing and offering to sell computer data from RAPCO. The computer data included computer-assisted drawing ("CAD") information required to obtain certification of several components as identical to parts for which RAPCO held certification. RAPCO stored all of its drawings and manufacturing data in its CAD room, which was protected by a special lock, an alarm system, and a motion detector. Further, the number of copies of sensitive information was kept to a minimum and surplus copies were shredded. Although engineers and drafters knew how to access the CAD room, the court held that RAPCO took "reasonable measures" to keep the information secret because the employees needed access to perform their jobs.

Garbage

One person's trash may be another person's treasure, but not in cases of economic espionage where "reasonable measures" are taken to keep the information secret and the information is used for an economic benefit. In Novell, Inc. v. Weird Stuff, Inc., Novell, a company engaged in developing, manufacturing, and distributing various types of computer hardware and software, sued Mark and Rick Gold (the "Gold Brothers") and Weird Stuff, Inc. for trademark infringement, copyright infringement, and false designation of origin in connection with its NetWare software. NO. C92-20467 JW/EAI, 1993 U.S. Dist. LEXIS 6674 (N.D. Cal. May 14, 1993).

The Gold Brothers were in the business of salvaging and reselling discarded software. They admitted to retrieving 1,700 NetWare software disks from a dumpster located behind the manufacturing facility of Novell's manufacturer. The retrieved disks were sold to Weird Stuff, which was not an authorized reseller of Novell's NetWare software. Subsequently, Weird Stuff entered into a contract with a computer company for over 70 times the amount that Weird Stuff paid for the NetWare software. The contract could be canceled if the disk could not be upgraded, because Weird Stuff was aware that Novell's cooperation was required for an upgrade. Novell learned of the disks when the computer company inquired about upgrades and an internal audit revealed that the serial

numbers of the disks should have been scrapped. The court found no genuine issue as to any material facts and granted summary judgment on Novell's claims for trademark infringement, copyright infringement, and false designation of origin.

Hiring Away

Competitors frequently hire away employees from companies to gain the employee's knowledge while working for competitors. Typically, the employee's knowledge relates to industry standards, which can be legitimately transferrable, but an employee's or executive's knowledge of critical or proprietary information can cross the line. In Magnesita Refractories Co. v. Tianjin New Century Refractories Co., Magnesita Refractories Company ("Magnesita") alleged, among other things, that its former employee, Donald Griffin, misappropriated its trade secrets in violation of the DTSA. No. 1:17-CV-1587, 2019 U.S. Dist. LEXIS 32559 (M.D. Pa. Feb. 28, 2019).

Griffin held several positions supervising the research and development of Magnesita's products related to refractory materials for producers of cement, glass, steel, and other metals. As a term of employment, Griffin acknowledged receipt of and agreed to Magnesita's Code of Ethics, which extensively defines confidential information and prohibits distributing confidential information to third parties. Magnesita alleged that during his assignment abroad as Technology Director, Griffin made contact with the Foreign-based co-defendants, one of whom owned a subsidiary located in the U.S. that competed directly with Magnesita. Following Griffin's return to the U.S., he retired from Magnesita and allegedly forwarded trade secrets and confidential information to his personal email, in addition to copying propriety information to an external drive before his retirement. Griffin was subsequently hired by the co-defendants. After learning that Griffin had not fully retired, Magnesita uncovered the forwarded e-mail. The parties settled the case before trial.

Intellectual Property Theft

IP theft includes the theft of technical documents and drawings, source code, pricing sheets, manufacturing processes, customer lists, and marketing strategy. Unauthorized access to these materials can be the result of cyberattacks or an employee copying the information. In 2001, a judge ordered that software company Avant! Corp. pay $195 million in restitutions to rival software company Cadence Design Systems. See Cadence Design Sys. v. Avant! Corp., 253 F.3d 1147 (9th Cir. 2001). Cadence and Avant! competed in the field of integrated circuit design automation, which enables computer chip designers to place and connect tiny components on a computer chip. Among other things, Cadence accused Avant! of stealing code provided by four senior employees who left Cadence and formed Avant! in 1991.

In 1995, a Cadence engineer discovered an error in Avant!'s software that was similar to a bug that they had inadvertently created several years earlier. Subsequently, Cadence contacted the Santa Clara County District Attorney, which executed a search of Avant!'s headquarters and seized, among the items, a log that showed line-by-line copying of the Cadence source code in 1991 by Stephen Wuu, a former Cadence employee and Avant! founder.

In the State of California v. Wuu, et al., No. 206394 (Cal. Super. Ct. Santa Clara Cnty. Dec. 16, 1998), Wuu was sentenced to two years in prison, three years of probation, and fined $2.7 million. Wuu received the harshest sentence, in part, because he took Cadence's source code in 1991 while employed with the company and modified small parts of the code to compete against Cadence. Another co-founder of Avant!, Yuh-Zen Liao, was sentenced to one year in prison, three years of probation, and fined $2.7 million. Eric Cho, another co-founder of Avant!, was sentenced to one year

in jail and fined $108,000.

Trespassing property

Industrial espionage can also involve obtaining company information by entering the physical premises or files of a company. The unauthorized access of company information can involve a current employee or an outsider. In E. I. du Pont deNemours & Co. v. Christopher, the Fifth Circuit Court of Appeals affirmed the trial court's determination that DuPont alleged a cause of action for the misappropriation of trade secret under Texas law. 431 F.2d 1012 (5th Cir. 1970). DuPont alleged that Rolfe and Gary Christopher (the "Christophers") were hired by an unknown third party to take aerial photographs of its new plant construction. Sixteen photographs of the DuPont facility were taken by an airplane circling over the plant, and later developed and delivered to the third party. The Christophers refused to disclose the identity of the unknown third party, so DuPont filed suit, alleging that the photographs taken by the Christophers showed the plant designed to produce methanol by its secret process. The Fifth Circuit held that aerial photography of plant construction is an improper means of obtaining another's trade secret and permitted the proceedings to continue.

While a separate article will discuss in greater detail methods to legally and practically protect your company from industrial espionage, basic steps to take to reduce risks include: limiting the access of outgoing employees to confidential information; immediately performing an audit of the confidential information that a former employee had access to in order to determine whether the information was downloaded or copied; and requiring outgoing employees to declare that they have not downloaded any company information or have any company information in their possession.

National Law Review, Volumess XII, Number 130