A Primer on Industrial Espionage

How Corporate Spies Steal Trade Secrets

Industrial Espionage: A Prologue

Imagine you're the CEO of a midsize company. Your goal is to outmaneuver the competition and snag a significant share of the market. Your firm might achieve this by delivering a useful product or service that consumers feel is worth the price. You're not the only company doing this, so you might also opt for savvy positioning, an extensive advertising campaign, an aggressive sales strategy, or some combination thereof.

You're not a giant in the field, but your company offers a viable alternative. Year after year, your firm is taking a larger market share. And your R&D department is on the verge of making your product more reliable and user-friendly—any breakthrough could be a real game changer.

You wonder what would happen if the competition beat you to the development or knew your company's strategy for introducing the improved product to the market. You've heard of industrial espionage but now you wonder: *How real is the threat?*

Industrial Espionage Defined

The word "espionage" calls to mind some high-stakes theft of classified information, executed by shadowy agents versed in sophisticated spycraft. The reality of industrial espionage is usually much less glamorous.

First, the definition: "Espionage" is the theft of secrets; therefore, industrial espionage is the theft of business secrets, or trade secrets. In order for industrial espionage to be a crime, business secrets must have legal protections—and they do. Trade secrets enjoy one of the broadest definitions in intellectual property law.

According to *18 U.S. Code § 1839,* a trade secret is essentially any information that the owner (1.) takes reasonable measures to protect and (2.) has actual or potential economic value.

The *Universal Trade Secret Act*, which has been adopted by most states, defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process" that the owner has taken steps to keep secret and which has potential economic value. Its economic value derives, in part, from "not being generally known to, and not being readily ascertainable." In other words, a trade secret must be something that is *not common* knowledge or readily deducible from public sources.

Trade secrets are an interesting species of intellectual property for several reasons: They have no statute of limitations; their scope is quite broad; and the law exacts significant sanctions for misappropriating them. A secret recipe for fried chicken, a computer schematic, the blueprint of a manufacturing facility, a marketing strategy, or a list of clients could all qualify as trade secrets if their owners took pains to keep them secret.

Federal law under *18 U.S. Code § 1832* of the *Economic Espionage Act of 1996* makes the interstate misappropriation of trade secrets a criminal offense punishable by up to ten years in prison and a five million dollar fine. If theft of the trade secret benefits a foreign government or agent, then the offender could face up to fifteen years in prison per *18 U.S. Code § 1831*.

Think those penalties are high? Check out the stakes: A 2013 report by the Commission on the Theft of American Intellectual Property revealed that intellectual property theft costs the U.S. economy $300 billion a year.

The Modus Operandi of the Industrial Spy

In classic espionage, spies are insiders who give one country's secrets to another. They may be moles on the inside or defectors who trade information for money or residency.

The dynamics of industrial espionage parallel that of the classic international spy's game. But often, the mechanics are far more mundane: A former employee accepts a position with a competitor or directly competes with a former employer, using privileged knowledge of the former employer's business to gain a competitive advantage.

There are, of course, differences. Whereas defectors or moles are nearly universally viewed as traitors and fully aware they're committing a crime, many former employees who share their ex-bosses' secrets may not realize they're breaking the law. Unlike betraying one's country for profit, climbing the career ladder (by whatever means necessary) is socially acceptable behavior—which may be why so many ex-employees fail to grasp the illegality of giving up a former employer's trade secrets.

Indeed, federal law does criminalize the theft of trade secrets; however, most cases are brought by civil action in state courts. Many of these cases involve allegations against former employees who went to work for competitors or established their own businesses in direct competition with their former employer. In these cases, the employer claims that the former employee is using their company's trade secrets to benefit their competition. Courts often do recognize the misappropriation of trade secrets and the violation of non-compete agreements and grant relief for these types of cases.

While most industrial espionage is low-tech, unsophisticated, and perpetuated by people who likely don't know they're committing a crime, plenty of industrial spies have stolen secrets with their eyes wide open, motivated by the huge advantage conferred by inside knowledge.

Here's an overview of some of the more sophisticated methods of the accomplished industrial spy:

Poaching Key Personnel

Competing companies may try to recruit people with knowledge of proprietary information by offering them a big salary bump, large consulting fees, or outright bribes. In a case pending in the U.S. District Court of Eastern Virginia, *DuPont Inc. v. Kolon USA Inc.*, DuPont alleges that Kolon stole trade secrets related to the production of Kevlar™ by hiring several former DuPont employees, including the primary developer of the material.

Kolon's defense is that the information on Kevlar's™ production is available from public sources. Meanwhile, the companies are fighting it out in civil courts.

Staking Out Trade Shows

Trade shows have long been a source of competitive intelligence. According to the Office of the National Counterintelligence Executive, trade shows are also prime targets for foreign intelligence services engaged in economic espionage.

Trade shows present opportunities for identifying key personnel, hacking data devices, and coaxing information out of unsuspecting attendees. In a 2011 trial, MGA Entertainment Inc. claimed that Mattel employees used pretexting to get into MGA's toy-fair showrooms and steal data about its products. A California jury awarded MGA a $172.5 million verdict, which was later overturned.

Then MGA sued Mattell for serious money. In a civil case pending in California (*MGA v. Mattell*), MGA alleges that Mattell spent years stealing product concepts, advertising information, and price lists from MGA at trade shows. MGA is seeking one billion dollars in relief.

This decade-long, billion-dollar legal battle all started as a copyright dispute…over MGA's popular line of Bratz™ dolls.

Dumpster Diving

Police and detectives have long known to look in the garbage when something smells fishy. A 1997 article in the *Yale Law and Policy Review* by Harry Wingo argued that there was an ambiguity in the law over dumpster diving when applied to trade secret cases, calling it an "ethical blind spot." Wingo argued that the law should consider dumpster diving an act of espionage.

If there is no privacy in the garbage, then one might conclude that there are no secrets in the garbage.

Today, the legal status of dumpster diving for corporate intelligence remains ambiguous. A 1988 Supreme Court decision, *California v. Greenwood*, held that there was no reasonable expectation of privacy in garbage left outside in the curtilage.

The legal definition of a trade secret requires *an effort to make and keep the secret*—i.e., without the effort, there is no secret. If there is no privacy in the garbage, then one might conclude that there are no secrets in the garbage.

It's a muddy and dangerous situation for the business that doesn't securely shred their papers.

Elicitation, Pretexting, and Human Engineering

Elicitation

Sometimes the easiest way to get information is to simply ask for it. It's rude, after all, to deny a polite inquiry. The FBI even has a flyer about the tactic—"*Elicitation Techniques*"—which warns about the dangers of polite conversation.

The pamphlet defines elicitation as "the strategic use of conversation to extract information from people without giving them the feeling they are being interrogated…Conducted by a skilled collector, elicitation will appear to be normal social or professional conversation. A person may never realize she was the target of elicitation or that she provided meaningful information."

Imagine, for instance, that you're an engineer enjoying an evening off at your favorite bar, when you overhear people—seemingly, a couple of clueless students—wildly understating the performance specs of a piece of tech you helped design. You are incensed, and eager to set them straight. Do you correct them? Should you engage in conversation because of your shared interests, and offer them the benefit of your superior knowledge?

"A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit those," says the FBI flyer. "Natural tendencies an elicitor may try to exploit include…a tendency to correct others (and) a desire to appear well informed, especially about our profession."

That overheard conversation might just be a trap set by a corporate spy.

Pretexting and Human Engineering

A tactic related to elicitation is pretexting—essentially, lying about your identity or status in order to get information.

In Kevin Mitnick's book, *The Art of Intrusion*, Mitnick describes this scenario: a private investigator calls a bank pretending to be an author. His goal is to get basic information about which service they use to check the banking history of potential clients. He also wants to learn the industry jargon so he can sound knowledgable when discussing that service.

Once the investigator learns the name of the company—CreditChex—he calls the bank back and pretends to be a CreditChex representative. In one call, the investigator is able to get the bank's account number with CreditChex and learn which number the bank's employees call when performing a bank history check.

The investigator then uses that information to call CreditChex, now posing as a bank employee, and uncovers personal information on an account holder. The purpose: to search for any potential hidden assets the subject might have stashed in that bank.*

The information security industry calls these psychological tactics *human engineering*. Academics, security consultants, and security executives widely acknowledge the weakest link in security is the human element—psychology. Thus, human engineering threatens even the most advanced security features.

*(*note: "The Gramm-Leach-Bliley Act makes it a crime to obtain customer information of a financial institution by means of false or fraudulent*

statements to an officer, employee, agent or customer of a financial institution." —Identity Theft and Pretext Calling, Board of Governors of the Federal Reserve System)

Hacking

A report by the Office of the National Counterintelligence Executive points to several growing vulnerabilities for U.S. companies which may "create new opportunities for malicious actors to conduct espionage": namely, the proliferation of connected mobile devices, and the trend toward storing information in the cloud.

Stealing sensitive information remotely through cyberspace can be particularly appealing to potential corporate spies because of the low cost and relatively low risk of detection. The report names several potential adversaries: other private companies, academic and research institutions, foreign nationals, and even foreign intelligence services.

Foreign Intelligence Services

According to the industrial espionage report cited above, "China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of US economic information and technology."

In March of 2014, a Californa engineer named Walter Lian-Heen Liew was found guilty of conspiring to steal trade secrets from DuPont and sell them to a Chinese state-owned company for more than $20m.

Liew reportedly solicited the recipe for a chloride-route titanium dioxide whitening process (used in Oreo cookie fillings, paints, and plastics) from a DuPont engineer and sold the information to several Chinese companies. He was convicted of violating the *Economic Espionage Act of 1996*. "The theft of America's trade secrets for the benefit of China and other nations poses a substantial and continuing threat to our economic and national security," said an assistant attorney general, quoted in this FBI report.

ABC News called this conviction a "shot heard around the world." "It's a message to foreign countries they can't spy on the U.S.," a former U.S. prosecutor told *ABC*.

photo by Toby Oxborrow

Since the collapse of the Soviet Union, the former USSR's intelligence services have also refocused their efforts on acquiring commercial technology, motivated by "the belief that the global economic system is
tilted toward US and other Western interests at the expense of Russia," says the Office of the National Counterintelligence Executive report.

According to Hedieh Nasheri in his book *Economic Espionage and Industrial Spying*, the threat comes not just from geopolitical adversaries but also from long-term allies. France, Japan, Israel, and Germany also spy on American businesses, according to a 1998 paper published in the *Public Administration Review* by Edwin Fraumann of the FBI.

Fraumann claims these intelligence services pursue American trade secrets aggressively, using sophisticated methods such as surveillance, wiretapping, employing prostitutes for the purpose of blackmail, bribery, planting moles, and soliciting employees with fake job offers in order to interview them.

Private Spies

In 1999, Oracle initially rejoiced when the U.S. government went after its rival, Microsoft, for supposed anti-trust violations. But when an "independent" nonprofit started buying

high-dollar ads that turned public opinion in favor of Microsoft, Oracle hired a private investigations company to look into the "nonprofit."

Oracle's investigations efforts made headlines when the PI agency allegedly tried to buy trash from maintenance staff employed by the organization it was investigating. (The custodial staff declined the offer and reported the incident.)

By outsourcing the spying, corporations might find themselves less interested in ethics than in results.

There's a potential ethical pitfall in hiring a private investigations agency for corporate intelligence work: It lets corporations off the hook, in a sense—by reducing their liability. If a corporation's in-house investigators and competitive intelligence personnel engage in industrial espionage, the corporation is clearly liable. However, that liability isn't so clear-cut if the corporation hires an outside investigator to collect information and the investigator happens to uncover trade secrets. Which means that by outsourcing the spying, corporations might find themselves less interested in ethics and legal restraint, and more interested in results, at any cost.

Epilogue

As that midsize company CEO, what do you do when a key engineer from your biggest competitor, disgruntled with his current employer, offers to jump ship and work for you? It might be risky to hire him, but aren't you just a little more than interested to know the circumstances of his disgruntlement? Is there turmoil inside the competition's ranks? Perhaps the competition knows that you're close to releasing an improved product. Do they have a counter-strategy to combat your potential market advantage?

The disgruntled engineer surely has insight into these problems. You might not be able to hire him outright, but imagine how much information you could get from interviewing him. What could it hurt? After all, if he has a noncompete and nondisclosure agreement, those are his responsibilities, not yours. Right?

Just a little bit of inside information could make big differences in strategy, market share, and profit margins.

What would you do? What would your competitors do?

About the author:

Kevin Goodman is a freelance researcher and writer. He has a master's degree from Skidmore College with a focus in cognition, culture, and communication. He also has a graduate certificate in criminology from the University of Massachusetts, Lowell.

His primary academic interest is the psychology of belief and its interrelationship with deception. Kevin enjoys making wine, being outdoors and exploring whatever he finds curious. He lives near Bloomington, Indiana, with his wife and two daughters.

Visit the ASP Website: http://www.advancedsecurityprotection.com/services/technical-surveillance-countermeasures-tscm-debugging