



Corporate Spying

An Overview



With the boom in informational and technological advancements in recent years, there comes the good and the bad—the bad being more susceptibility to the theft of confidential and valuable information that can ultimately lead to a substantial monetary business loss or competitive disadvantage in the marketplace.

Espionage (defined)

According to the Merriam Webster Dictionary *Espionage* is defined as:

*the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company (industrial espionage) [from the French *espionnage*, from *espionner* to spy]*

Although the term sounds very *cloak and dagger* and makes us think of cold war era spy's in the US and former USSR, it has recently been used more to describe what companies all over the world and in most industries, are doing to each other. With the US and most world economies in a prolonged slump, corporate spying is seen as a way to gain a competitive edge, a market advantage or perhaps to embarrass or put a competitor out of business.

Types of Espionage

There are various types of spying or reconnaissance that are intended for commercial purposes, rather than solely for national security objectives and they have become more widespread in recent years with globalization and fair trade initiatives.

Industrial espionage is the “misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret.”

Economic espionage is the “misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent.” Misappropriations in both events can include stealing, copying, transmitting, buying, or even destroying trade secrets. Both cases are considered criminal acts under the Economic Espionage Act of 1996 (EEA).ⁱ The EEA was the first federal act to define and enforce penalties for misappropriation and theft of trade secrets. The law makes it illegal to steal trade secrets, as well as copy, duplicate, sketch, download, or communicate them to others.

According to an estimate by the Federal Bureau of Investigation (FBI), billions of dollars are lost every year to foreign and domestic competitors who intentionally target business intelligence



from US industries and technologies as well as commercial technologies by exploiting information and trade secrets. The FBI notes that foreign competitors criminally seek intelligence by recruiting insiders or establishing “cover” business relationships or by the more general acts of bribery, theft, wiretapping, covert surveillance and cyber invasion.ⁱⁱ

Corporate espionage is international in scope, and transpires between businesses, companies, or corporations. One of the most significant misconceptions is that high-tech criminals, sophisticated spies, and computer hackers conduct it. More often than not, corporate espionage is carried out by simple and preventable measures. With so much focus today on computer security, corporate spies can more easily slip into an unlocked office or neglected conference room to tap into information sources like the trash can or a vulnerable telephone. Or secrete a small listening device that can be remotely triggered, in a company’s executive conference room or an executive’s office. As a general rule of thumb, a good spy will always look first toward the path of least resistance.

Two things exacerbate the problem: lack of awareness of general security practices by employees and lack of proper valuation of intellectual property and company information. One example is draft documents, which are often discarded with less caution than finalized products, but may contain the same advantageous hard facts and numbers for a company.

Intellectual Property

Economists estimate that US intellectual property is worth about \$5 trillion, which is nearly half the country’s economy. They also estimate that the theft of trade secrets may cost companies \$300 billion per year.

Since 1991, every few years the American Society of Industrial Services (ASIS) has been conducting a survey “Trends in Propriety Information Loss” to report on the challenge for American businesses to protect their information property from traditional and emerging foreign threats. The most recent version from August 2007 states that businesses felt a range of financial impact from theft of proprietary information, from as little as less than \$10,000 to as high as more than \$5.5 million. In the past, Fortune 1000 companies have reported losing information and property valued at \$53 to \$59 billion for a one year period. The report highlights one of the key problems with intellectual property and proprietary information. Although “as much as 75 percent of the market value of a typical US company may reside in intellectual property assets,” the value of these assets is not always well established or 100%



known, so it is likely not well protected at the level proportionate to its value or relevance to the company.ⁱⁱⁱ

The current ASIS report also identifies some major trends in the industry, such as:^{iv}

- Information assets in all formats (paper, electronic, oral, prototypes, and models) are being targeted for possible compromise
- Deliberate actions of current and former employees are a *primary threat* to proprietary information
- Exploitation of trusted relationships—including those involving vendors, customers, joint ventures, and subcontractors/outsourced providers—is a threat to proprietary information

To give additional perspective on intellectual property crimes, in the fiscal year 2010, the FBI opened no less than 190 new Intellectual Property criminal investigations, 66 of which were related to trade secret theft. Also, the Department of Justice contributed nearly \$4 million to state, local, and law enforcement agencies in the same year to educate, deter, and enforce on prosecuting Intellectual Property crimes.^v

Insider Threat

It is easier to detect and protect against outsider stealing company information than it is to control the insider or the employee with legitimate access to business data. Insider theft may occur for personal gain, or to collect information or products to benefit another company or country. According to the FBI, there are a number of personal motives that may increase the likelihood for an employee to spy against an employer, including: greed or financial stress, anger or revenge over a workplace incident, work disagreements or problems, ideology or identification with a specific cause, displaced loyalty, vulnerability to blackmail, or pure thrill.^{vi}

Cyber Threat

Recent cyber-attacks indicate that cyber espionage is evolving and is a significant threat to companies and governments. For example, Lockheed Martin Corp, the largest defense contractor in the world and the Pentagon's number 1 supplier, fell victim to a cyber-attack on May 21, 2011. The company released a statement reporting that it had detected a "significant" attack on its communications network. They had detected the attack almost immediately and stopped it before any critical customer, employee or program data was lost. The incident is now being investigated by the Department of Homeland Security and the Department of



Defense to determine the extent of the attack. Additionally, an analysis of available data will be performed to find ways to mitigate further risk.

Lockheed uses a mobile security system produced by RSA, the security division of EMC Corp. RSA experienced their own breach of their network in March 2011, which had resulted in the theft of RSA data. Following the security breach, RSA had boosted security for its clients. The president of an information security company called NSS Labs, Rick Moy, said the initial attack on RSA most likely targeted RSA's customers, including governmental, military and financial organizations. Additionally, he reported that the original RSA attack had been followed by phishing and malware activities, seeking specific data, which signals that the attacks on Lockheed may have been carried out by the same hackers. Weapons makers like Lockheed are the latest organizations to be breached through cyber-attacks that have targeted other global corporations including Sony and Google. Fortunately, the attack on Lockheed's computer network had limited impact on the Department of Defense.

Acts in Place for Information Security

In addition to the EEA Act of 1996, the US Congress has enacted other laws to better protect corporate information. For example, the Sarbanes-Oxley Act (SOX) was enacted on July 30, 2002 in response to a number of major corporate scandals, most notably the Enron scandal, which resulted in investors losing several billions of dollars when share prices of affected companies collapsed. After the resulting loss of public trust in the US securities markets, SOX was created to provide a more stringent system of checks and balances for organizations. SOX improves the accounting and information management procedures that companies need to follow per the Securities and Exchange Commission (SEC). Additionally, SOX requires that companies develop and implement appropriate protocols in the retention, management, control, and disposal of documents.

Also, the Gramm-Leach-Bliley Act (GLBA), or the Financial Services Modernization Act of 1999, was created to ensure banking and financial institutions put in place a formal information security plan outlining how the entity secures and plans to continue to protect clients' personal private information.

Best Practices

According to the FBI, there are numerous steps a company can take to help protect against the threat of espionage, which include:^{vii}



1. Recognize an insider/outsider threat may exist
2. Note and value trade secrets
3. Put in place a comprehensive plan for protecting trade secrets and proprietary information
4. Secure physical and electronic copies of valuable information
5. Keep intellectual knowledge to “need-to-know” only in the office
6. Enact and information security plan and train employees on its specifics

MSA Investigations and its parent company MSA Security, provides a complete line of services to help you secure your important information against the threat of espionage, including Technical Surveillance Counter Measure (TSCM) “bug” sweeps. Please contact us at the phone number below, or through our website, and we would be glad to discuss with you how we can help.

ⁱ Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2008.

ⁱⁱ FBI, Counterintelligence/Economic Espionage, <http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage>

ⁱⁱⁱ ASIS Trends in Proprietary Information Loss Survey Report, 2007

^{iv} Ibid

^v “DOJ Steps Up Prosecutions for Trade Secret Theft,” The National Law Journal, 31 January 2011

^{vi} FBI Publication, The Insider Threat

^{vii} FBI, Counterintelligence/Economic Espionage, <http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage>