CORPORATE ESPIONAGE - CASE REVIEWS

Industrial espionage and electronic eavesdropping surveillance is growing at a phenomenal rate. The U.S. State Department estimates that there are over 700,000 eavesdropping devices sold each year. The State Department also reports that over 6,500 incidents of industrial espionage occur in the United States each year with an average economic impact of $1.25 million per incident. Unfortunately, these surveys and estimates do not include the over 600,000 businesses in the U.S. with more than 20 employees or the 98,000 companies with more than 100 employees.

In the FBI's pending case load for the current fiscal year, economic espionage losses to the American economy total more than $13 billion. As the FBI's economic espionage caseload is growing, so is the percentage of cases attributed to an insider threat, meaning that, individuals currently (or formerly) trusted as employees and contractors are a growing part of the problem. The insider threat, of course, is not new, but it's becoming more prevalent for a host of reasons, including:

- Employee financial hardships during economic difficulties.
- The global economic crisis facing foreign nations, making it worth the risk to steal technology rather than invest in research and development.
- The ease of stealing anything stored electronically, especially when one has legitimate access to it.

HISTORY:

1800's - In the 1800s, Britain had a thirst for tea, a brew monopolized by China. So the London-based East India Co. hired Scottish botanist and adventurer Robert Fortune to smuggle the tea's plants, seeds, and secrets out of China and into British-ruled India. Disguised as a Chinese merchant, he succeeded, and within his lifetime the production of tea in India surpassed China's. It was the "greatest single act of corporate espionage in history," according to Sarah Rose, author of For All the Tea in China.

CASE STUDIES

IBM Vs Hitachi - 1980 - This case of computer company corporate espionage was dubbed "Japscam" by the press - perchance in hopes of a made for TV movie or perhaps a computer game! In 1981 Hitachi mysteriously came into possession of an almost full set of IBM's Adirondack Workbooks. It seems that the fact that they contained IBM design documents full of IBM technical secrets and were prominently marked FOR INTERNAL IBM USE ONLY didn't prompt Hitachi to return them.

IBM counterintelligence staff and FBI personnel worked tirelessly until the arrest of several IBM officials proved the fruits of their labor. Hitachi settled out of court, and paid IBM a sum that has been reported as US$300 million.

Kodak Vs Harold Worden - 1995 - Pensioner power was something that Harold C. Worden obviously believed in. After completing 30 years with the Eastman Kodak Corporation he retired and promptly set up a consulting company, brokering the services of over 60 other retired Kodak employees. Not content with simply bringing with him several thousand confidential documents relating to the machine, he also convinced his successor to provide him with even more.

He was sentenced to one year in prison and fined $30,000, only a little more than he had received for the stolen information, which Kodak held to be worth millions of dollars.

Opel Vs Volkswagen - 1997 - It's bad enough for a company when their top executives jump ship - but imagine how it must have felt for Opel when their chief of production moved to rival Volkswagen and was followed by not one, not two, but seven other executives. Opel cried industrial espionage - over an alleged missing bundle of confidential documents - in response to which Volkswagen parried with accusations of defamation.

The four-year legal battle was resolved in 1997 when Volkswagen agreed to pay General Motors, the parent company of Opel, $100 million and place an order for over $1 billion's worth of car parts. In the end, the companies agreed to one of the largest settlements of its kind: GM would drop its lawsuits in exchange for VW's pledge to buy $1 billion of GM parts over seven years. In addition, VW was to pay GM $100 million.

Avery Dennison Corp Vs Pin Yen Yang (Four Pillars) - 1997 - Pin Yen Yang, President of Four Pillars, a Taiwanese company that makes and sells pressure-sensitive products, and his daughter Hwei Chen Yang, were arrested and charged with a smorgasbord of offenses related to industrial espionage against Avery Dennison Corp, a major US adhesives company. In 1999 they were convicted of paying an Avery Dennison employee a reported $150,000 for proprietary information received over an eight-year stretch, causing the company tens of millions of dollars in losses. Sticky business indeed.

Gillette Vs Steven Louis Davis - 1998 - Steven Louis Davis was sentenced to 27 months in prison and ordered to pay $1.3 million in restitution for his theft of trade secrets from Gillette. Davis worked for Wright Industries, a company which Gillette had contracted to assist with a new shaving system. Steven Louis Davis, an employee at Wright Industries Inc., a designer of fabrication equipment that was hired by Gillette, faxed or e-mailed drawings of the new razor design to Warner-Lambert, Bic, and American Safety Razor. Davis pled guilty to theft of trade secrets and wire fraud and was sentenced to 27 months in prison. He told the court he stole the information out of anger at his supervisor and fear for his job

Cadence Design Systems Vs Avant - 1999 - In the early '90s allegations came to light that Avant!, a Silicon Valley software company, had stolen code from a rival company, Cadence Design Systems. This became more than a simple case of unscrupulous business practices when prosecutors filed charges and, in 2001, Avant! was ordered to pay $182 million in restitution plus interest and fees, for a total of $200 million.

Worse still for Avant!, the closing of the criminal case meant that Cadence was finally able to proceed with its own civil case. Not content with a paltry $200 million, Cadence settled with Avant!, who'd since been bought by Synopsys, for a further $265 million. If a company could figure out a way to arrange this kind of profit, they wouldn't be doing badly.

Microsoft Vs Oracle - 2000 - It's not all rosy at the top. Larry Ellison, the head of Oracle and at one time the second richest man in the world, has no shame about his covert monitoring of rival, Microsoft chief and one-time richest man in the world, Bill Gates. In fact, Ellison has no regrets about his 2000 efforts to expose Microsoft's funding of various public interest groups.

His hired detective's efforts are said to have involved bribing the cleaning staff at Microsoft's Washington office in order to lay their hands on documents. Oracle Chief Executive Larry Ellison said it was doing its "civic duty" by hiring a detective agency to investigate groups that supported Microsoft.

Oracle said it sought evidence that the groups were receiving financial support from Microsoft during its antitrust trial. Oracle admitted their detective agency had tried to buy trash from two cleaning women at the Association for Competitive Technology, a research group that Microsoft backed.

Procter & Gamble Vs Unilever - 2001 - P&G denied Fortune Magazine's allegation that their operatives pretended to be market analysts. In 2001, Procter & Gamble admitted to a spying operation, alleged to have been carried out over 6 months, on its hair-care competitor Unilever.

Their cunning plan, which P&G referred to as an "unfortunate incident," included going through Unilever's trash in search of documents, although if Unilever habitually throw away full documents entitled "Super Secret Product Information That Will Crush P&G" their days as an industry leader are numbered. The two companies reached an agreement, and P&G has pledged not to use any of the information it gained in product development.

DuPont Vs Michael Mitchell (Kolon Industries) - 2005 - Michael Mitchell worked on the marketing and sales of Kevlar for DuPont until he was fired in 2006. Unwilling to sign on to unemployment with his tail between his legs, instead he offered to provide his services to Kolon Industries Inc, a Korean form which just happens to be one of two companies that manufactures fibers that can tough it out with Kevlar in the toughness stakes.

After emailing his new bosses confidential information on Kevlar, he went back to old colleagues at DuPont to find out more. Unsurprisingly, DuPont executives found out about this less than cunning scheme and notified the FBI. Mitchell was sentenced to 18 months in prison and ordered to pay DuPont over $180,000.

Hewlett-Packard - 2006 - Hewlett-Packard's board became ensnared in a scandal in 2006 after the company spied on its directors, reporters, and employees in a probe to ferret out the source of boardroom news leaks. Investigators hired by the company obtained personal phone records by posing as reporters and company directors. They also trawled through garbage and followed reporters. As a result, then-Chairman Patricia Dunn, who approved the spying, was fired. HP also agreed to pay $14.5 million to settle an investigation by California's attorney general, $6.3 million to settle shareholder lawsuits, and an undisclosed amount to settle a case filed by journalists at the New York Times and Business Week, which is now owned by Bloomberg.

Starwood Vs Hilton - 2009 - Starwood rocked the hospitality world when they accused household name Hilton of industrial espionage based on Hilton's employment of 10 executives and managers from Starwood. Starwood's accusations were centered around luxury brand ideas, with the former head of Starwood's luxury brands group alleged to have downloaded "truckloads" of documents before leaving for the bigger firm.

In 2010, the two groups reached a settlement that required the Hilton group to make payments to Starwood, as well as refrain from developing a competing luxury hotel brand until 2013. In 2010, Starwood settled its case and said Hilton was ordered to make sure "the conduct that occurred does not occur again

News International phone-hacking scandal — dubbed "**Hackgate**", "**Rupertgate**", or "**Murdochgate**" - 2010 - Britain‘sphone hacking scandal. Prosecutors announced that Rebekah Brooks, who ran Murdoch’s British newspapers, and Andy Coulson, who served as Cameron’s communications advisor, were among those charged with illegally tapping into the cell phones of celebrities, politicians and other public figures while working at the now-shuttered News of the World tabloid.

Over a six-year period starting in the fall of 2000, Brooks, Coulson and five of the other suspects conspired to break into the phones of more than 600 people, prosecutor Alison Levitt said. On the list of victims: actors Brad Pitt, Angelina Jolie and Jude Law, singer Paul McCartney, soccer player Wayne Rooney and at least one Cabinet minister.

The alleged hacking was part of the News of the World’s relentless pursuit of sensational stories and extended as far as accessing the voicemail messages left on the phone of a 13-year-old kidnapping victim who was later found slain.

Amid the uproar that followed, Murdoch shut down the 168-year-old tabloid, issued a public apology and was hauled before Parliament for questioning. Top executives at News International, the British arm of his giant News Corp., resigned in disgrace, including Brooks, once one of the Australian-born media magnate’s most trusted lieutenants.

CYBER ATTACKS

Hackers stole proprietary information from six U.S. and European energy companies, including Exxon Mobil, Royal Dutch Shell, and BP, according to investigators and one of the companies. McAfee said the attacks resulted in the loss of "project-financing information with regard to oil and gas field bids and operations." It also said the attacks, dubbed Night Dragon, originated "primarily in China" and began in November 2009. Marathon Oil, Conoco Phillips, and Baker Hughes were also hit, according to people familiar with the investigations. Hackers targeted computerized topographical maps worth "millions of dollars" that locate potential oil reserves, said Ed Skoudis of InGuardians, a security company

Cyber Attacks - In what was described as one of the largest Cyber Attacks, more than 70 companies, governments, and nonprofit organizations were hacked by spies beginning in 2006, according to security company McAfee, which didn't name the perpetrator in its report. Dell Secure Works, another security company, traced the same attacks and pointed to China as the source of the attacks. Victims included a U.S. real estate company, a New York media organization, defense contractors, a South Korean steel and construction company, the International Olympic Committee, and the World Anti-Doping Agency. Hackers took information from some of the victims over a period as long as two years

Google & Cyber Attacks - In a January 2010 blog post, Google disclosed that it detected the previous month a highly sophisticated cyber attack originating from China that resulted in the theft of its intellectual property. The company said evidence suggested that a primary goal of the attackers was to access the Gmail accounts of Chinese human rights activists. Google said a wide range of companies were also targeted, including those in the finance, technology, media, and chemical industries. "This is a big espionage program aimed at getting high-tech information and politically sensitive information," James A. Lewis, a cyber and national security expert at the Center for Strategic & International Studies, told the Washington Post

THE REALITY

There is a common misconception about corporate espionage: many view the practice as a concern for only businesses with sensitive, government-related intelligence dealings. But this could not be further from the truth.

As you can see from these examples, corporate espionage is a very real aspect of business. Since corporations do their best to downplay their various scandals, this issue doesn’t receive the amount of attention and concern it deserves. For every action there is a re-action. Your best one is to be proactive. It's your business and Core Group is here to ensure it stays your business.