MINDSTAR SECURITY & PROFILING

Concierge Security Report
September 2016
Volume 2, Issue 9

Industrial and Economic Espionage

Introduction

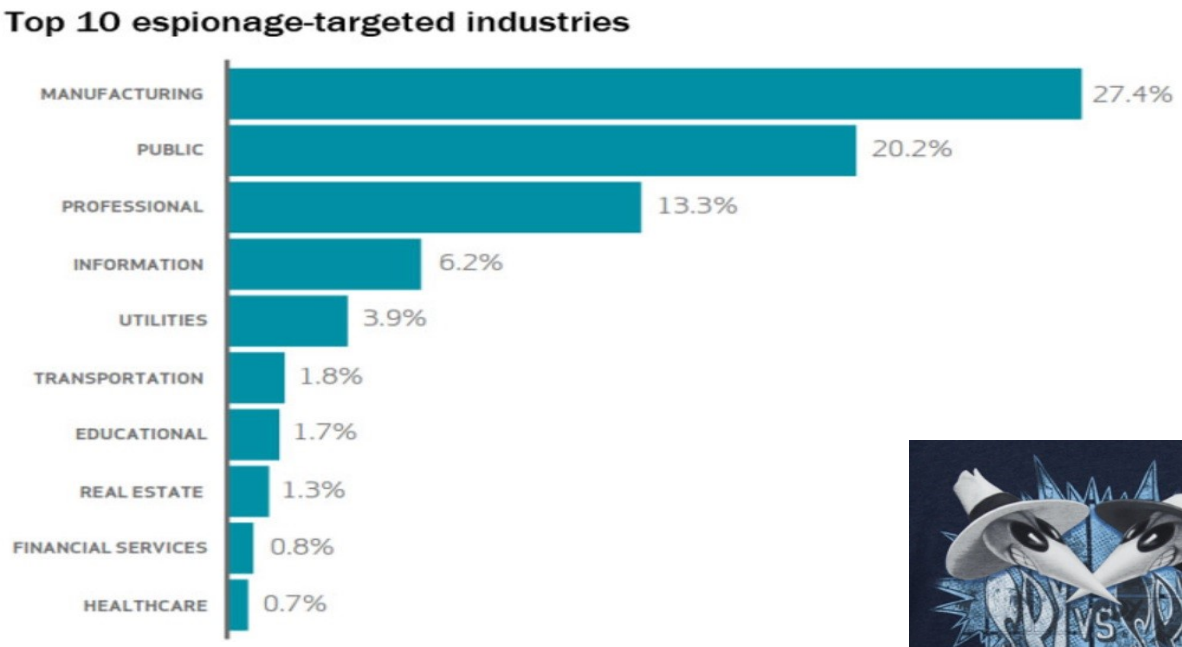
Industries within the United States spend more money on research and development than any other country in the world. The effort and resources required to develop unique products or processes that give businesses an edge over their competition is substantial. When someone infiltrates these companies and steals that edge, the company is left reeling. Whether the trade secrets are stolen by a rival company within the same country or by a foreign country, the victim company can often experience a loss of revenue, loss of jobs, damaged reputation, loss of future research and development budget, or even an interruption in the production of their product(s).

The Justice Department says that the scale of China's corporate espionage is so vast it constitutes a national security emergency, with China targeting virtually every sector of the U.S. economy, and costing American companies hundreds of billions of dollars in losses -- and more than two million jobs. In a worst case scenario, the theft of trade secrets can result in the victim company going out of business. The tactics used by corporate spies spans a vast array of methods or tradecraft. In some cases, the spies use "old fashioned" human intelligence gathering techniques. But more so, the theft of sensitive information is being conducted through hacking, cracking and other technical means. Over the past decade, more than 120 cases of malicious insider crime involving classified national security information were identified by the CERT Insider Threat Center.

The loss of trade secrets, confidential information, or theft of research is called industrial or economic espionage. While these terms are often used interchangeably, there are a few differences that will be discussed in the following report. Both of these forms of espionage have been around for a long time but are becoming more and more prevalent in recent years. This issue costs the American economy billions of dollars every year and can even be considered a national security risk. The following reports is intended to provide you with a basic understanding of industrial and economic espionage, as well as tips and recommendations on how to avoid falling victim to this growing problem.

Inside this issue

Industrial Espionage.....2
Economic Espionage.....2
Little to No Focus on Spying.....2
Competitive Intelligence.....3
Espionage Tactics.....3
The Defense Industry.....3
Economic Espionage by China.....4
Business Travelers.....4
Spying - Even in Baseball.....5
Prevention.....6
Stingray Technology.....7
Recommendations.....6-7



Source: Verizon's 2015 Data Breach Investigations Report

Industrial Espionage

Industrial espionage is the covert and often times illegal practice of investigating competitors to gain a business advantage. The target of the espionage could be a trade secret like proprietary software or formula, information about a business plan, or any number of other sensitive secrets held by a company. In many cases, corporate spies are simply seeking any information that their organization can exploit in order to gain a competitive advantage over other companies in their market.

Industrial espionage is distinct from competitive intelligence, which is the widely used business tactic of gathering and analyzing publicly available information on competitors and an industry in order to gain a competitive advantage.

Economic Espionage

Economic espionage is very much like industrial espionage, but instead of it being Company A versus Company B within the same country, it is the targeting of a key business or trade secrets by a foreign country. Many of the tactics used in industrial espionage parallel with those related to economic espionage. Foreign governments conduct economic espionage in order to bolster their economy by pulling valuable trade secrets from foreign countries and placing them within their own, generating wealth and spurring development and growth of businesses within their borders. Proving the foreign connection in court is often difficult, and cases that start out as economic espionage often end up prosecuted as theft of trade secrets. Each of these crimes is covered by the Economic Espionage Act of 1996 and can carry lengthy prison sentences for individuals and significant fines for organizations.

Historically, economic espionage has targeted defense-related and high-tech industries. But according to the FBI, many recent cases have shown that no industry, large or small, is immune to this threat. The FBI suggests that ANY company with a proprietary product, process, or idea can be a target and any unprotected trade secret is ripe for the taking by those who wish to illegally obtain innovations to increase their market share at the victim company's expense.

Little to No Focus on Spying

Many organizations do not specifically provide training, education or monitoring programs which focus on espionage. And it is not surprising - to some degree. Tradecraft and the sources and methods spies use to gain access and information are not taught in business school and not discussed in the board room (unless there is a compromise). No one may know what tradecraft might look like or how to detect or prevent it. Even security experts who have degrees in criminal justice or information science do not necessarily have coursework or exposure to the methods of tradecraft. In fact, many former Federal law enforcement officers do not specialize in tradecraft, but rather have expertise in investigative tactics and the corresponding legal parameters of preventing and solving crimes.

Espionage in the Defense Industry

This summer, Gregory Allen Justice, a Boeing employee and satellite specialist was arrested on charges of espionage. He was caught selling secrets to a Russian spy who was actually an undercover FBI Agent.

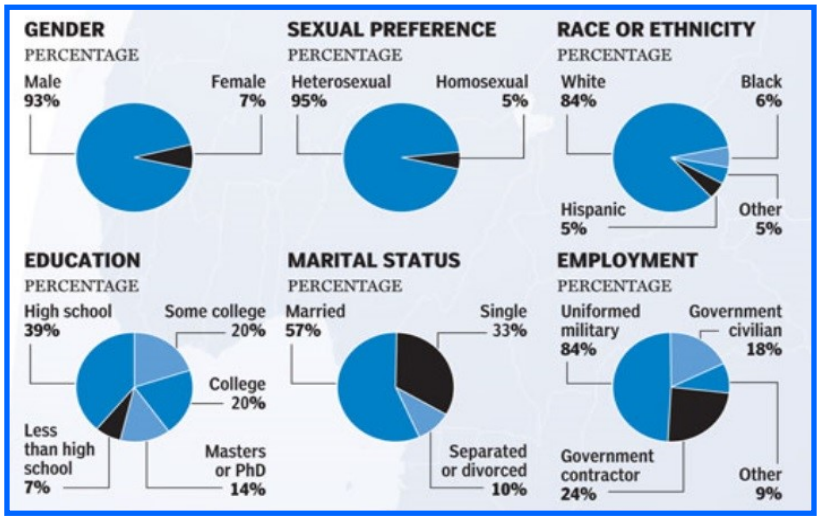
There is some speculation on why and how Mr. Justice became a would-be spy but some of his behaviors provide some insight to his motivations:

- Allegedly began spending thousands of dollars on online "how to spy" training courses.
- Researched the "sovereign citizen" movement which believes that U.S. citizens are immune to any form of federal law.
- Obsessed with spy movies and TV shows such as the Bourne series and The Americans.
- Passed over several times for a promotion and complained that he is doing the work "of people two levels above him."
- Claimed he had a seriously ill wife and the money would be used for her care – although some of the money went to another woman.

Competitive Intelligence

Before getting into the tactics used by corporate spies, it is important to understand what industrial espionage IS NOT. Competitive intelligence, or CI, is the process of collecting and analyzing information about a competitor's strengths and weaknesses in a legal and ethical manner in order to enhance business decision-making. Competitive intelligence means different things to different people within an organization. For example, to a sales representative, it may mean advice on how best approach a key decision maker while pursuing a lucrative contract. To a high ranking executive, it may mean unique marketing insights to gain market share against competitors.

Competitive intelligence can be grouped into two main types: tactical and strategic. Tactical CI often focuses on a short term goal and seeks to provide information into issues like capturing market share or quickly increasing revenue. Strategic CI focuses more on long-term issues like identifying risks and/or opportunities that may present themselves in the future. The ultimate end goal of competitive intelligence is to help make better decisions and enhance organizational performance. The information gained through this process is done so legally, often with publicly available information obtained via the open source Internet.



Who Are the Spies? Former CIA Officer, Richards Heuer, analyzed 150 cases of espionage since the late 1940's and his data presents some interesting demographics.

Source - National Post Press Service

Industrial and Economic Espionage Tactics

The number of tactics used by spies are only limited, by some degree, to their imagination and ingenuity. Current technologies, such as miniature cameras, small storage devices, drones, micro-recorders and the like can make the spy's job much easier as these devices are easily attainable at almost any online or brick-n-mortar store. Some of the very basic tactics include:

Physical Breach: Spies will sometimes physically breach their targets property. In cases like this, spies can search files, go "dumpster diving" or search through waste baskets, or even access unattended and unprotected computers in order to copy files or install spying software.

Corporate Networks: Increasingly, spies are getting a foothold into a company via the company's corporate network. Often times, a targeted attack is conducted to gain their initial network access and is followed by an advanced persistent threat (APT) in order for them to continue collecting information.

Insider Threats: An industrial spy can be an insider threat, possibly someone that has gained employment with a company with the sole intent of spying or even a disgruntled employee who decides to sell private corporate information for personal gain or revenge.

Social Engineering: Other spies may work from a distance, infiltrating a company via social engineering and tricking employees into providing them with important (and private) privileged business information.

Business Travel - Beware of Spies

Most business travelers do not have complete awareness of the threats of espionage. Today, the risks are greater and more people are being targeted. Everyday thousands of executives, scientists, consultants, and defense contractors are passing through train stations, airports and other public venues. Each business person most likely carries proprietary documents, contact lists and electronic files in the latest electronic devices.

Corporate spies target those devices and the data on them. Therefore, there are things that business travelers should be aware of or avoid all together:

- In flight social networking – many airlines are offering apps and the ability to network with those around you on your flight. This is the equivalent of wearing a sign around your neck that says, "*Hey, my name is Sam, I work for the Acme Corporation and I want to talk to strangers*." Just do not do it.
- Shoulder surfing – attain screen blockers for your laptops, that way people sitting behind you cannot see everything you are typing or reading.
- "Loud-talking" – if you have to take a call in a public place, speak quietly or find an area that has some privacy.
- Complimentary WiFi services (e.g., airports, hotels, cafes) – use your own MiFi apps or services. Do not trust services that are offered to the public.

Economic Espionage by China

According to the NSA, recent years have seen 700 Chinese cyber-attacks designed to steal corporate or military secrets in the United States. The FBI also reported a sharp increase in economic espionage cases aimed at U.S. business last year, with the vast majority of attacks coming from China. During a FBI briefing last summer, the agency said that they had observed a 53% increase in economic espionage cases over the past year. The theft of trade secrets over the previous few years is believed to have been responsible for the loss of hundreds of billions of dollars. Corporations that had been targeted during that time included companies like DuPont, Lockheed Martin, U.S Steel, Westinghouse Electric and Valspar, most of which have since worked closely with the FBI to better protect their intellectual property.

After that briefing last summer, the FBI launched a nationwide campaign intended to warn industry leaders of the serious risks they face from foreign countries looking to steal trade secrets. A big part of this campaign came from government officials that believed the loss of trade secrets was more than just an economic issue. Special Agent Bill Evanina, the head of the National Counterintelligence and Security Center, suggested that economic security was directly related to national security and that economic espionage creates a serious risk to national security. The FBI has actually been using many of the same tools they use to identify and track terrorists to identify and track economic spies. A CNN article, also from last summer, mentioned a survey conducted by the FBI in which half of the 165 private companies surveyed claimed to have been victims of economic espionage. Of those companies that believed they had been victims, 95% of those attempts were believed to have originated with individuals directly associated with the Chinese government.

"Despite the passage of the Economic Espionage Act almost twenty years ago, if recent statistics are to be believed, there is so much trade secret thievery going around that the United States finds itself in the midst of an epidemic of economic espionage."

Source: University of Miami Law Review, May 1, 2016.

Just two months after last summer's FBI briefing and the start of their campaign to spread awareness of economic espionage, the United States and China came together to pledge that neither government would conduct or condone economic espionage in cyberspace. The pact also called for ministerial or Cabinet-level processes aimed at ensuring compliance by each government. It is believed that that Chinese were rattled by President Obama's multiple threats of economic sanctions and the criminal indictments that United States leveled against five Chinese military officials for economic cyberespionage.

While many officials did not put much faith that the Chinese would actually change their ways and take measures to curb all of the economic spying they were conducting, it appears that they have been abiding by the September pledge. Private U.S. security executives and government advisors suggests that breaches attributed to China-based groups had plunged by almost 90% over the last year and that the most dramatic drop occurred right around last September's meeting between President Obama and Chinese President Xi Jinping. Kevin Mandia, who founded Mandiant and recently took over as FireEye's chief executive, suggests that several factors seemed to be behind the Chinese shift. He cited embarrassment from a 2013 Mandiant report that harshly blamed the Chinese government for rampant spying and the 2014 indictment of the five Chinese military officers. Officials within the Obama administration appear to not yet be ready to proclaim that China is fully complying with the agreement but did state that the most recent report was promising and that U.S. officials are still conducting their assessment on Chinese compliance.

Economic Espionage by China, continued

Just because hackers and economic spies have toned down their attacks on U.S. companies over the past year or so does not mean that these threat actors have just quit spying and found new lines of work. Security experts have seen a sharp rise in attacks being carried out by hackers and spies linked to the Chinese government against Russian government agencies and technology firms, political groups and corporations in India, the Mongolian mining industry, and other targets in Japan and South Korea. The Chinese government appears to simply have re-allocated their espionage resources to different targets for the time being. It is impossible to predict how long this fragile pact between the United States and China will last but U.S. companies currently have a great opportunity to shore up their defenses in order to be better prepared for the likely scenario where the Chinese turn their sights back on U.S. industry.

The red dots indicate the locations of more than 600 corporate, private and government targets of Chinese cyber espionage that were attacked between 2010-2015.

Source: http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211

Corporate Espionage - Even in Baseball

Nothing is sacred...not even apple pie or baseball. In late 2015, a bakery in San Francisco was burglarized. The only thing stolen were 230 recipes for muffins, frostings, cakes, and pies. The cash, iPads, and expensive equipment were left untouched. Rival pie and cake makers clearly found it important enough to break & enter and burglarize the bakery for its trade secrets.

In January 2016 the former St. Louis Cardinals scouting director, Chris Correa, pleaded guilty to hacking the Houston Astros' computer database. The St. Louis Cardinals gained access to internal discussions about Houston's trade negotiations, proprietary statistics, scouting reports, and playbook strategies. The information attained provided insights into some of the inner operations of the St. Louis Cardinals and was deemed the first documented case of corporate espionage in professional baseball.

The theft of information from the Houston Astros was due to, in part, a problem with their passwords. The FBI's investigation stated that Correa was able to gain access using a password similar to one used by a Cardinals employee who "had to turn over his Cardinals-owned laptop to Correa along with the laptop's password" when he was leaving for a job with the Astros in 2011. While the password was not an exact match, there was a pattern to the formation of the new password - but not enough to prevent the intrusion. Out-processing procedures should include a focus on changing all physical and technical ingress methods including badges, keys, locks, usernames, and passwords.

Preventing Industrial & Economic Espionage

Business advantages are becoming more and more vulnerable to theft by corporate spies, whether foreign or domestic. This problem is costing U.S. businesses hundreds of millions of dollars and is viewed by many as a physical security threat to the country. While economic espionage from China appears to have declined recently, there is no way of knowing how long that threat will remain dormant and the threat of industrial espionage by domestic competitors remains a concern. That is why it is critical that companies adopt a defensive posture against this threat. The following recommendations were taken from imgsecurity.net and from threat assessments conducted by Mindstar Security. We hope these tips provide some insight on how to go about better protecting your company's trade secrets and other sensitive data.

"The World Economic Forum (WEF) says a significant portion of cybercrime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot."

Recommendations

Identify your Company's Sensitive Information - It is important to identify exactly what the company's trade secrets are. By properly evaluating the company's intellectual property, they will be more able to establish priorities and allocate security resources to better protect the most vital secrets. In short, you cannot protect your secrets if you do not know what your secrets are.

Identify the Threats - Before companies develop strategies to fight against industrial or economic espionage, they need to fully understand what organizations present the largest threat to them. A company's competitors may pose the most obvious danger but it should be kept in mind that visitors, customers, business partners, hackers, activist groups, and foreign nationals are all potential threats and should be considered when creating the security plan.

Shore Up Physical Security - Companies should make sure the physical security of their offices, equipment, and infrastructure are sound. This means carefully setting up surveillance systems, securing entry points, and hiring (or contracting) specialized security personnel. It is especially important that companies identify the most sensitive information and locations and ensure that these areas are given an extra layer of security.

Establish Detailed Policies for Controlling the Flow of Information - Companies should establish policies on what information certain employees can share inside and outside the workplace. They should also establish specific procedures for control, reproduction, and storage of sensitive information. Significant attention should be paid to what is being shared over the Internet, email, and social media sites. Additionally, companies should develop procedures for the proper disposal of physical waste like paper documents and IT hardware. This prevents the loss of information to "dumpster diving" and other more physical forms of spying.

Train & Educate Employees - Having the previously mentioned policies is not enough to safeguard information. Employees need to be trained to understand the policies and follow the proper procedures regarding the flow and protection of information. Companies should conduct periodic training and awareness campaigns in order to make sure employees fully understand how to protect information, as well as the threats they face with regard to espionage. Employees need to understand that the threat of espionage is both external and internal. It is also important that employees can identify suspicious behavior or activity.

Management /Security Training - Managers and security specialists should be trained, to some degree, in tradecraft. Many security specialists have expertise in investigation, physical security, and operational security, but may not have an applied background in methods of tradecraft used by those committing espionage.

Compartmentalize Information - This point is very important in protecting secrets. Not all information needs to be accessible to every employee. This is why information, even that which may seem insignificant, should be compartmentalized on a need to know basis. Every senior manager or executive may not need to know every technical detail about the company's operations. Companies should put in place detailed policies to segregate which employees have access to certain information, with careful attention given to the employees who have access to the company's most sensitive trade secrets.

Stingray Technology

One way spies can attain confidential information from cellular devices is to use what is called Stingray technology. In broad terms, Stingray is a fake cell tower. More specifically, it is a small electronic device that mimics cell tower signals, thus tricks your phone into connecting to it instead of the legitimate cell tower. The Stingray device does this by sending out a signal that is stronger than the signal of a real tower. The Stingray also connects itself to the real cell tower so that devices that are now connected to the Stingray can still operate normally – but everything you do is passing through the Stingray. Therefore would be spies are able to:

- Obtain data that has been stored on your phone;
- Track and locate through access to the GPS data;
- Conduct denial of service; and,
- Intercept communications content.

Case evidence suggests that these devices have been used for industrial espionage.

Recommendations, continued.

Conduct Background Checks and Monitor Employees - Companies should conduct background checks on any employees with access to sensitive information, including janitors, caterers, and groundkeepers. Companies should try to identify any possible factors that could make a particular employee more prone to illegally disclosing information, such as fraud or theft history, drug use, etc. It is also a good idea to carry out periodic "refreshers" or secondary security evaluation sometime after the employee has been initially vetted for employment.

Establish Employee Exit Procedures - Companies should develop comprehensive employee exit policies. This means that all employees should be required to sign a nondisclosure agreement and be reminded of this agreement upon leaving the company. Also, companies should be aware that most cases of intellectual property theft by employees occur during their last month of work. This is why it is imperative to make an employee's exit as smooth and resentment-free as possible. Companies may also think about limiting the access to information for employees that are expected to leave the company in the near future.

Beef Up Cyber Security - It is important for companies to maintain a strong cyber-security position. This is particularly important in defense of potential economic espionage from the Chinese, who have been known to employ cyber-attacks as a means of accessing corporate networks. Systems should look both outward and inward, as monitoring internal networks may uncover suspicious activity and record the transmission, copying, and accessing of sensitive information. Companies may consider utilizing specialized software to protect critical information, monitor activity and access, and ultimately help prevent data loss.

Establish Clear Crisis Management Protocols - It is important that companies develop contingency plans and crisis strategies in the event of intellectual property theft. Companies should attempt to assess the potential damage caused by the theft of certain pieces of information or trade secrets and develop specific response plans for each. The company's losses in terms of competitiveness and reputation should be considered as well. It is a good idea for companies to have a legal strategy should a case of industrial or economic espionage take place. Finally, "war gaming" or "disaster scenarios" should be run so that companies can identify any problem areas of their processes/ protocols and work to fix them.

Believe it Can Happen - No one wants to think that their company is being targeted or that their employees are part of the threat. But it happens to great companies, run by great people. Employees who are familiar with the inner workings of a particular organization are being recruited by foreign agents in exchange for large amounts of cash.

"...trade secret and data theft are projected to double by 2017. "

Mindstar Security & Profiling specializes in security solutions for family offices, high profile/high net worth executives, and their families. Our customized focus includes the security trifecta of Internet/Social Media Safety, Physical Security and IT Security.

1001 Sycolin Rd SE, Suite 1A
Leesburg, VA 20175

Phone: 703-404-1100
Fax: 703-404-5549
www.mindstarsecurity.com
E-mail: info@mindstarsecurity.com

MINDSTAR
SECURITY & PROFILING