THE IMPACT OF INDUSTRIAL ESPIONAGE AND THE VALUE OF PROTECTING A COMPANY'S INTELLECTUAL PROPERTY RIGHTS

Brian Cazzell, Realize, Inc.; Jeffrey M. Ulmer, University of Central Missouri

Abstract

Industrial espionage is a viable threat that companies need to safeguard themselves against. The objectives of this study were to examine the nature of this crime and the methods used to commit the crime, to provide examples of how this crime impacts the U.S., to describe the laws that protect intellectual property, to describe the steps a company should take to decrease its vulnerability, and to provide engineering technology students with a primer on industrial espionage. Finally, the study concluded with the development of a reference list for managers and engineering technology students who will someday become managers regarding steps to reduce their own risk.

Introduction

Does a mother's secret recipe book have value? What about secret recipes that have been handed down through multiple generations? Perhaps such a secret recipe contains "Grandma's chocolate chip cookie recipe" or "Aunt Edna's homemade lasagna" recipe; special recipes that have been perfected over the years with love and care. Suppose someone bakes those items for a luncheon at work or a social gathering for friends and after the food is tasted by others, someone asks for the recipe. Hesitantly one might say, "Sorry, it's a secret family recipe." Much to the disappointment of others, the individual has basically preserved what is rightfully theirs. It may seem trivial but, in essence, that individual has just protected their intellectual property rights.

On a larger scale, what if the secret recipe was something that could be used as value? For example, a person decides to bake and sell Grandma's cookies as described earlier for a profit. Now everyone is clamoring to get their hands on those delicious goods. If the secret recipe was ever leaked to the public, profits, and the individual's future as a cookie baker, would soon be over. This scenario has been depicted many times in national television ads for Bush's Baked Beans©. In the commercial series, the Bush's loveable family dog, Duke, constantly threatens to publicize the family's secret recipe for making the beans. It may seem comical to the viewer but, in reality, the result could be devastating for the Bush's baked bean business. Whether the information is leaked or stolen, it is still classified as industrial espionage, which is a very serious crime that is punishable by law.

According to the Office of the National Counterintelligence Executive, industrial espionage is defined as, "The theft of sensitive information that has independent economic value and that the owner has taken reasonable measures to protect, regardless of the perpetrator's country of origin or whether a foreign government agent can be linked to the theft" [1].

As a business owner or manager, or student who will someday be a manager, the following should be known:

- What type of information these criminals are willing to steal.
- What avenues they will take to steal it.
- The impact of industrial espionage on businesses.
- How to protect a company from becoming a victim of this crime.
- What laws protect a business from this crime and the challenges courts face when applying them.

Trade Secrets Defined

In order to effectively combat this crime, one must first understand what type of information criminals are searching for, i.e., trade secrets. The definition of a trade secret according to the U.S. Department of Labor's Occupational Safety and Health Administration website is information that "may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it" [2]. In addition, it is a trade secret if it is used in a repetitive process and directly related to a formula such as a list and amount of raw materials used in a product, a specific manufacturing process that is not common knowledge, or even a list of clients.

As a reference, patents document a machine or process improvement to an existing device and convey ownership to the patentee. Trademarks are designs, symbols or word-

phrases owned by a person or a company. Lastly, copyrights are very similar to trade secrets, but they are designed to protect the original work of a person, whether the idea or product is a song, book or photograph [3]. Basically, trade secrets can range from how a product is manufactured to the actual ingredients which are used to make the product. Some classic examples of trade secrets are the formula for Coca-Cola© or the Colonel's Secret Recipe of 11 herbs and spices at Kentucky Fried Chicken©. Most businesses in a market economy develop their own trade secrets to give their product a distinction among their competitors' products. One of the biggest reasons companies need to keep trade secrets from their competitors is to protect and maximize their future profits. Trade secrets are also critical in developing and growing a company's market share by giving its products or services a differentiating quality from its competitors.

Methods of Industrial Espionage

Now that we know what type of information is being stolen from companies, let's look at how it is being stolen. Once a person has decided to commit industrial espionage, there are a few avenues he can take to steal this information. Usually, the crime is committed by an employee working for the company who already has access to the trade secrets. Since many larger companies have their own research and development divisions, many employees may have first-hand knowledge of new products coming out onto the market. In most cases, employees with strong ethics and loyalty will be bound to confidentiality agreements required for working in that division or on a project. However, an employee with questionable ethics may not feel equally bound to those agreements so he may decide to sell information to an employee of a business competitor for a large monetary payment. The consequences of this action may end up costing a company millions of dollars in lost profits as a result of diminished market share due to rival companies introducing an identical or substitutable good or service. In addition to the lost profits of future sales, a company may also lose the money it invested in researching and developing the new product. In most cases, larger companies with their own R&D divisions spend millions or possibly billions of dollars each year in researching and developing new products. For example, the drug manufacturer Pfizer reported over two-thirds of their cash flow is reinvested into research and development of new products [4]. With so much time and money invested in developing products, companies have to find a way to protect their investment by keeping their "secret formulas" to themselves. This type of industrial espionage would be hard to detect since there would be no signs of forced entry onto the company's premises.

A recent article in the Washington Post titled "Data Theft Common by Departing Employees [5]" described just how bad this trend is really getting. According to the article, a survey was conducted by the Ponemon Institute to determine the relationship between data theft rates by employees who have either been laid off, fired or changed jobs in 2008. According to the research, nearly 60% of 945 survey respondents admitted to stealing email lists, non-financial business information, customer contact lists, employee records and financial information. Of those 60% who admitted to stealing this protected information, the majority indicated they did so "in order to leverage a new job" [5]. Figure 1 is a summary of the different types of information commonly stolen by the 567 out of 945 survey respondents that indicated they had stolen protected information from their company [5].

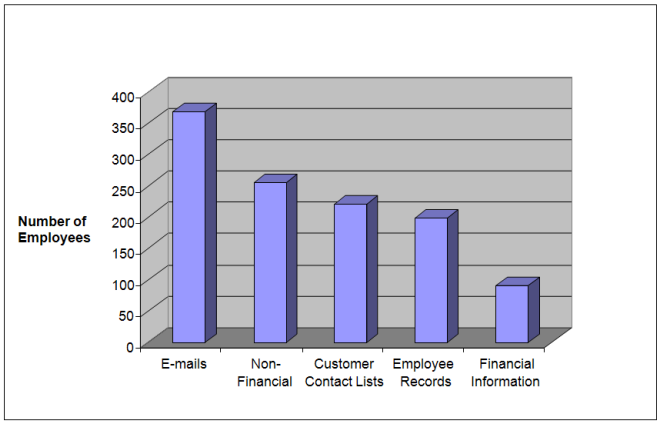

Figure 1. Data Theft Categories

In addition to theft by an employee, other thieves may be lurking on the outside of a company. This is a direct result of the rapid technological growth in affordable surveillance equipment. Now, with the help of a few simple gadgets, it is becoming easier for someone to commit industrial espionage from the outside of a company without being caught. Items that were once considered only available to law enforcement—such as phone taps, electronic eavesdropping devices, computer hacking software, and other professional spy gear—are now available to anyone looking for it. With the help of these simple gadgets, thieves could easily monitor phone conversations, hack into the company's IT network and gain access to files, or even utilize video monitoring devices to videotape confidential or secret activity within the company.

Impact of Industrial Espionage

According to the American Society of Information Security (ASIS), as much as 75% of a company's market value is

held in intellectual property assets or, in other words, their trade secrets [6]. In August, 2007, ASIS released a survey report entitled "Trends in Proprietary Information Loss" [6]. The survey has been conducted every two to three years since 1991 by ASIS in collaboration with the Office of the National Counterintelligence Executive. The purpose of the survey is to study and track the impact of industrial espionage on U.S. businesses. According to the 2007 report, which was based on survey results conducted in 2006, 144 companies that responded reported losses ranging from less than $10,000 to more than $5.5 million per company [6]. That's quite a staggering amount, especially in the current state of the U.S. economy. Size of the company does not appear to matter, as it appears that any company is prone to this type of theft. The report indicated that approximately 10% of the survey respondents were companies with an annual revenue of less than $10 million and, on the other hand, approximately 7% were companies with greater than $10 billion in annual revenue, while the greatest segment, 20.8% of respondents, were companies whose annual revenue was between $1 billion and $4.9 billion. According to the U.S. Commerce Department, "intellectual property theft is estimated to top $250 billion annually...and also costs the United States approximately 750,000 jobs, while the International Chamber of Commerce puts the global fiscal loss at more than $600 billion a year" [7].

One example of the impact of industrial espionage occurred between 1999 and 2001 at Corning, Inc., a manufacturer of electronic components for consumer electronics and telecommunication systems. During this time an employee discovered blueprints of a future liquid crystal display (LCD) project in the waste bin at a warehouse. After closely examining the documents, he realized there was a potential for selling them to an Asian competitor, PicVue, for a profit. He contacted PicVue's president and arranged for a meeting to discuss plans to sell the blueprints which contained the proprietary information. A deal was struck between the two and for the next two years the Corning employee continued to sell blueprints marked for destruction to PicVue for a small payment of $25,000. The crime might have gone on for several years but PicVue approached a third party developer, Saint-Gobain, who ironically was involved in the development process on the same blueprints with Corning. Concerned by this, Saint-Gobain contacted Corning to alert them of a possible case of trade secret theft. Corning consequently contacted the FBI who launched a full investigation. In the end, it was determined that the intellectual property stolen by the Corning employee was valued at approximately $100 million. When the trial went to court in 2006, the Corning employee pleaded guilty and was sentenced to 4 years in prison and fined $20,000. Additionally, PicVue was ordered to pay Corning $15 million in damages [7]. This problem could have been entirely avoided if Corning had instituted better follow-up measures to ensure their secret blueprints and documents were actually destroyed immediately instead of placing them in an unattended bin out in the open for other employees to find.

Steps to Mitigate Risks

With so many different areas to cover, it's hard to know where to start. However, a few basic guidelines should help drastically reduce the chance of a company being ripped off. First and foremost, training and educating employees about the consequences of leaking sensitive information about the company would be very cost effective and the least time consuming. The training may include having employees sign a proprietary document stating they are aware of the sensitive nature of the information they possess and the consequences of sharing it with anyone. Employees may also be trained in the importance of protecting their passwords to their workstation computers along with other simple steps to protecting information stored on them.

Second, all documents containing sensitive information can be moved to one central room and access to that room can be monitored by installing card reading devices on the door. This will allow a company to keep track of anyone who enters or exits the room along with the exact date and time of their entrance. This method may be costly and have a few drawbacks, but the company would still be able to maintain strict accountability for its records. As new biotechnology is being developed in this area, more reliable scanning devices are available that can be used to scan the employee's retina or fingerprint instead of a card which could be stolen or used by someone else. Automated Fingerprint Identification Systems (AFIS) are readily available. The Federal Bureau of Investigation (FBI) has an exhaustive list of approved and certified AFIS devices on its website [8].

Another easy way to protect a company's information is to ensure that employees are properly disposing of paper containing sensitive information. According to a California-based company known as Instashred Security Services, Inc. [9], many different types of forms should be properly shredded but are often overlooked; for example, forms that contain customer data, inventory records, proprietary programs, sales statistics and financial statements. Companies such as Instashred can be hired to securely remove any paper or media products containing sensitive information from a company and destroy them before heading off to a recycling bin, thus guaranteeing the information contained on the paper will be lost forever. These three steps should be used as a starting point but there are many other ways to protect a

company from industrial espionage that could be utilized depending on the size of a company's budget.

Legal Aspects of Trade Secrets

Trade secrets are considered intellectual property similar to copyrights, trademarks and patents; however, the laws that protect each of these are vastly different. Originally, trade-secret laws were developed as common laws in the 1800s, but the need for specialized legal protection of these property rights steadily increased over the past few decades. In 1985, the National Conference of Commissioners on Uniform State Laws drafted the Uniform Trade Secrets Act (UTSA), which has since been adopted by most states. This Act states that a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval [10]. In addition to the UTSA, Congress passed the Industrial Espionage Act in 1996. The primary role of the act is to "prohibit economic espionage, to provide for the protection of United States proprietary economic information in interstate and foreign commerce, and for other purposes" [11]. Combined, these Acts provide courts with guidance in determining how to apply trade-secret laws which differ from patent laws in that they address different, non-inventive subject matter and focus on conduct instead of technology" [12].

The task of applying these laws is not an easy one. Courts must first decide if proper ownership of a trade secret exists [13]. Ownership usually belongs to the person who created the formula, recipe or other process. Another factor courts must decide is what type of misappropriation has occurred; in other words, how the information was obtained or used [13]. In order to determine liability, courts must decide if a trade secret was sold or obtained as a result of someone spying, eavesdropping, or as a result of any other suspicious method. Courts must also consider if the person or company that obtained a stolen trade secret knew that the source of the information was not legally obtained. If the company knew the source was not legally procured, but proceeded to take the information from the source anyway, then both parties would be held liable. Once a court has determined if any of these actions apply to the case, it will have to award an appropriate level of compensation to the victims and punishment to the criminals. Compensation usually includes damages which are based on the actual loss caused by the misappropriation and the defendant's unjust enrichment [13]. If the act of stealing the information is determined to be spiteful or intentional, then punitive damages may be awarded to the criminal also.

Summary

Economically speaking, industrial espionage is wreaking havoc on the stifled global economy. With figures ranging from a few million to hundreds of millions of dollars lost each year by companies, to the startling amount of between $250 billion to $600 billion lost per annum in the U.S., it is hard to ignore the magnitude of this problem on the aggregate economy. Despite having a legal system that is capable of prosecuting these crimes, criminals are continuing to commit this act with the help of new technologies which make it harder to detect. Protecting a company from industrial espionage may seem like a daunting task, but three simple steps can be followed to decrease a company's risk of exposure to this type of crime as long as managers are willing to invest a little time and effort. Here is a list of common safeguarding practices:

- Educate employees to the risks by holding formal training sessions.
- Limit access to trade-secret information to only those who need to know.
- Destroy data or printed documents which contain trade-secret information immediately after it is no longer necessary to keep.

Finally, managers must always be on guard for new technology, which would make stealing trade-secret information easier and less detectable. By staying educated of new technologies and theft mechanisms, managers, employees and engineering students who may become managers someday, will be able to quickly identify any signs of suspicious activity in their organizations. This ability is a company's first line of defense in protecting itself from the crime of industrial espionage.

References

[1] Office of the National Counterintelligence Executive. (2004, February). Annual Report to Congress on Foreign Economic Collection and Industrial Espionage.

[2] Occupational Safety and Health Administration (OSHA). (2011, April). Regulations (Standards - 29 CFR) Definition of Trade Secret (Mandatory) - 1910.1200 App D.

[3] Jennings, M. M. (2006). *Business: Its Legal, Ethical, and Global Environment*. (7th ed.). Mason, Ohio: Thompson-West.

[4] Pfizer Australia Pty Ltd. (2008). General Facts – Research and Development.
[5] Krebs, B. (2009, February 26). Data Theft Common by Departing Employees. *The Washington Post*.
[6] American Society of Information Security. (2007, August). *Trends in Proprietary Information Loss: Survey Report*. Survey Report by the ASIS Foundation.
[7] Burgess, C., & Power, R. (2006, June). Secrets Stolen, Fortunes Lost: How economic espionage and intellectual property theft destroy businesses and endanger the global economy. *CSO*. Retrieved from http://www.csoonline.com/article/220889/industrial-espionage-secrets-stolen-fortunes-lost
[8] FBI Biometrics Center of Excellence. (2009, April). IAFIS Certified Products List.
[9] Singer, A., (1994, June). Instashred Aims to Prevent Industrial Espionage. *The Public Record*.
[10] National Security Institute (1985). Uniform Trade Secrets Act.
[11] National Security Institute (1996). Industrial Espionage Act of 1996.
[12] Miller, A., & Davis, M. (1990). *Intellectual Property Patents, Trademarks, and Copyright in a Nutshell*. (2nd ed.). St Paul, MN: West.
[13] Mallor, J., Barnes, A., Bowers, T., & Langvardt, A. (2004). *Business Law, the Ethical, Global, and E-Commerce Environment*. (12th ed.). New York: McGraw Hill.

Biographies

BRIAN CAZZELL is a Client Success Manager at Realize, Inc.. He assists engineers in planning and building rapid prototype (RP) models with stereolithography (SLA) and urethane casting processes during the pre-production stage of the product life cycle. He received a master's degree in Industrial Management from the University of Central Missouri. He retired from the U.S. Navy in 2009 where he most recently served as the Leading Chief Petty Officer of the VA/DoD Integration Support Team in Great Lakes, Illinois, and as a Certified Master Training Specialist at the Center for Naval Leadership in Ingleside, Texas. He is a member of the Society for Manufacturing Engineers. Mr. Cazzell can be reached at brian.cazzell@realizeinc.co

JEFFREY M. ULMER, Ph.D., is an Associate Professor of Engineering Technology and Industrial Management at the University of Central Missouri in Warrensburg, Missouri, teaching both undergraduate and graduate students. Ulmer is an American Society for Quality Certified Manager of Quality & Organizational Excellence and a Certified Six Sigma Black Belt. He is also a trained Lean Six Sigma Black Belt (from the Regal-Beloit Corporation) and has worked for 25 years in industry in the areas of product engineering, quality assurance / control, and production management. Dr. Ulmer may be reached at julmer@ucmo.ed