12-2014

The Economic Espionage Act of 1996: A 15 Year Review

Matthew T. Priebe
Grand Valley State University

The Economic Espionage Act of 1996: A 15 Year Review

Matthew Thomas Priebe

A Thesis Submitted to the Graduate Faculty of

GRAND VALLEY STATE UNIVERSITY

In

Partial Fulfillment of the Requirements

For the Degree of

Masters of Science

Criminal Justice

December 2014

Acknowledgements

I would like to thank all of those who have helped me complete this thesis. First and foremost, I would like to thank my committee members for working with me for over two years. Second, I would like to thank my parents, Bruce and Donna Priebe, as well as Heather Chuhran for supporting me while working towards the completion of this paper. Lastly, I would like to thank Marie Stuve for editing this paper in its entirety.

Abstract

It is estimated that the United States alone loses $300 billion annually to economic espionage. The purpose of the paper is to understand the occurrence and defining characteristics of economic espionage. This is accomplished through the series of proposed research questions related to the Economic Espionage Act of 1996. These questions include: occurrence rates, offender demographics, victim demographics, and victim-offender relationship. Archival data analysis of all 18 USC §1832 prosecutions from 1996-2011, will answer each proposed research question. The results will provide worldwide corporations with statistical support to help combat economic espionage. Specifically, descriptive statistics, such as mean, median, and mode, will be used to explain the nature and extent of economic espionage as defined under 18 USC §1832. Ultimately, this study found that economic espionage is a major problem for the United States, affecting a variety of classifications of companies.

Table of Contents

List of Figures and Tables

TABLES

FIGURES

Chapter 1: Introduction

Economic espionage and theft of trade secrets are a serious problem for United States' companies. For the purpose of this study, economic espionage is defined as the theft of valuable information from a company by an individual, or individuals, for personal advancement or a competing company's advancement. Economic espionage is specifically related to foreign transactions, meaning that the theft was committed to benefit a foreign entity (EEA, 1996). The occurrence of foreign espionage is increasing exponentially every year (Almeling, Whitney, Sapoznikow, Snyder, and Weader, 2010). Between 1994 and 1995, the number of cases investigated by the Federal Bureau of Investigation nearly doubled from 400 to 800 cases (Desmet, 1999). It is predicted that this trend will continue into the future and will double every couple of years, if not annually (Almeling et al., 2010).

A subsection of the Economic Espionage Act of 1996, and specific to this study, §1832 deals directly with the theft of trade secrets (EEA, 1996). Trade Secrets, as defined by the Economic Espionage Act, are any information which derive independent economic values by not being readily known to competitors (Goldstein, 2007). In other words, trade secrets allow companies to keep their products "secret" in order to reduce the number of competitors within the global market.

The United States is one of the most valuable nations in the world with intellectual property assets valued at over $5 trillion (Almeling et al., 2010). Intellectual property is often the result of one's creativity and can be a copyright, patent, trademark, trade secret, or brand name (Butler, 2005). This is estimated to be nearly half of the United States' economic worth. Economic espionage and theft of trade secrets are becoming a way of business (Crane, 2005). With such a large amount of the United States' equity invested in intellectual property, the

purpose of this paper is to understand the occurrence and defining characteristics of economic espionage. Equally important is the understanding of time investment that companies endure within the court process of foreign espionage cases. For example, a company may spend $1 million in legal and processing fees, which far exceeds a $200,000 profit from the stolen information. It is important to study this topic because of the increasing occurrence of foreign espionage. If foreign espionage continues to increase, companies will continue to lose out on economic prosperity. Also, the United States is often one of the most victimized countries due to the vast amount of intellectual property. Nearly $300 billion are lost annually due to the crime of foreign espionage (Almeling et al., 2010).

Chapter 2: Literature Review

History of Economic Espionage

Economic espionage and trade secret theft is not a new phenomenon. For example, it has been used since the invention of the wheel and throughout pre-industrial society (Coskun and Jacobs, 2003). Also, secrets for wheel making were stolen from the Roman Empire by the Celts, and simple techniques for making silk products were stolen from the Chinese by the Italians (Bergier, 1975). Not all acts of theft are needed to be so covert. Most acts of espionage are committed though simple activities, such as over-hearing a conversation, or observing a document in legal open spaces. In fact, in some instances of economic espionage and in some nations, competitors wanting to gain access to trade secrets would visit factories and shipyards to observe and steal manufacturing techniques (Davids, 1995).

Throughout history, a common method used to misappropriate trade secrets is the MICES (money, ideology, compromise, ego, and sexual entrapment) technique (Pacini, Placid, Wright-Isak, 2008). MICES is used to encourage individuals to steal trade secrets due to an alliance with a foreign nation, or different beliefs than those of the employer (Pacini et al., 2008). The United States also frequently engages in economic espionage. During the 1800s, the United States successfully stole trade secrets from Great Britain to increase prosperity of the American textile industry (Fialka, 1997). Francis Cabot Lowell traveled to Britain to spy on Britain's textile industry and steal water-driving cotton-weaving technology. Throughout history, the prevalence, sophistication, and value of losses have steadily increased due to MICES (Coskun & Jacobs, 2003).

Industrial society is at an even greater risk of economic espionage (Desmet, 1999). Due to the increase in technology, globalization, and the need for economic dominance, economic

espionage is steadily increasing (Coskun & Jacobs, 2003). Because of these increases, economic espionage "is the front line of a new world economic war" (Sepura, 1998, p. 128). Prior to the Cold War, the focus was on protecting military intelligence but has now shifted towards United States' corporations (Fraumann, 1997). In the post war era of today's society, there is no longer a need for the use of "war spies" in order to gain access to military secrets. The attention, therefore, has shifted towards becoming the leading nation in the international economic competition. As the Cold War came to an end, the "war spies" needed new employment (Minott, 2011). These old time spies of the Cold War did not just simply disappear (Maxwell, 1998). Many of them became employed by companies as corporate spies. They often become privatized and, "inaugurated Cold War II, the era of the global surveillance economy," (Maxwell, 1998, p. 138). With the increase in technology, globalization, and the need for economic dominance, companies have new, more sophisticated methods of obtaining intellectual property.

It is estimated that of the 173 nations worldwide, nearly 57 are actively seeking to steal trade secrets from the United States' corporations (Coskun & Jacobs, 2003). However, the United States is not the only targeted nation for trade secrets. Many other nations, such as China, Japan, and Israel, whose corporations hold value in the world market, are often victimized, too (Powers & Forte, 2007). This worldwide problem lead to the creation of the Economic Espionage Act of 1996.

Different Classifications of Assets

There are many ways in which a company or organization, can classify intellectual property in order to help safeguard information from becoming compromised (Goldstein, 2007; Hemphill, 2013). Patents, copyrights, trademarks, and trade secrets are all used to classify

intellectual property (Hemphill, 2013). These can be used in combination or in part, to better protect information from the criminal act of economic espionage.

First, patents are used to promote two objectives: to show product designs and to control the global market on the established product (Goldstein, 2007; Carte, 1998). Patents allow consumers to see product designs and goals of technological goods which promote investment and allow for the products to be sold at the lowest possible price (Goldstein, 2007; Carte, 1988). Patents protect the producer from a competitor building an identical product, therefore, reducing the likelihood of a competitive market. That is, no one else can produce the product with the same specifications unless the patent is revoked or removed (Goldstein, 2007; Carte, 1988). This allows for companies to keep costs low, as they do not have to compete for profits on a specific good. Within the application process for a patent, a company must provide and explain all details related to the product and its design (Carte, 1988). These records are then published publically and easily accessible for viewing by all, including corporate spies. During this process, a company must make sure the benefits of ensuring a patent outweigh the possible risks (Blakeslee, 2010; Carte, 1988).

Secondly, information classified under copyright is strictly related to all forms of expression (Goldstein, 2007; Epstein, 2004). A copyright simply protects written forms of expression, not ideas. At the initial installment of these laws, copyright proof laws were only directed at protecting written books, maps, and charts. It has most recently been expanded to include any and all forms of expression such as, novels, motion pictures, music, instruction manuals, bookkeeping forms, and computer programs (Goldstein, 2007). There is, however, one major lacking component under copyright law; it does not protect ideas. Copyrights differ from

patents in the essence that copyrights protect expressions, such as written materials, while patents protect products from being identically manufactured by a competitor.

Thirdly, trademarks are used to legally protect brands and its products from competitors who attempt to mock an original product (Kingston, 2006; Goldstein, 2007). Basically, a trademark is a word, symbol, or name used to identify the source of the product (Silber, 2008). Historically, trademarks were used to protect the consumer against market confusion pertaining to where the consumer good originated (Goldstein, 2007). In modern society, trademark law, "is to give legal force to the practice of brand extension, giving trademark owners' rights not only in the markets where their brands first acquired fame, but in other markets as well" (Goldstein, 2007, p. 28). This allows for a company like Coca-Cola to retain its name worldwide in multiple global markets without having multiple companies with similar names trying to replicate the actual trademarked brand of Coca-Cola (Goldstein, 2007).

Lastly, trade secrets are the most common way in which companies classify their intellectual information in order to protect intellectual ideas (Ronde, 2001; Pacini, Placid, and Wright-Isak, 2008). This is an important breakthrough because intellectual property law withholds protection from ideas (Goldstein, 2007; Epstein, 2004). Previously, a person's ideas were not protected against theft. Trade secrets allow for a person's or company's ideas to be protected from being stolen without any form of consent. Trade secrets are the most all inclusive way to protect intellectual property. Through the use of trade secrets, companies can better safeguard their intellectual property (Epstein, 2004). It should be noted, however, that in order for trade secret law to be enforced, the victimized entity must have engaged in reasonable actions to maintain secrecy (Quinto & Singer, 2012).

Trade secrets and trade secret laws are essential parts of the corporate realm. Nearly 80% of the value of the Standard & Poor's 500 companies consist of intangible assets (Goldstein, 2007; Pacini et al., 2008). Of that 80%, nearly 70% were created from ideas individuals had gained from previous employment. The most important aspect to classifying information as a trade secret is that it becomes protected from theft during the research and design phase of development (Goldstein, 2007). Trade secret cases are often the least likely to result in a criminal trial because companies fear that during the discovery process of a trial, the competitor will be able to gather even more information about the intellectual property due to the prosecuting company having to disclose any and all relevant information.

Although the above stated techniques are often used to protect a company's assets, they are not 100% effective (Goldstein, 2007). These techniques can be used in combination or in part in order to reduce the likeliness of becoming a victim of economic espionage. While patents, copyrights, and trademarks help to protect against established goods and services, trade secrets are essential to help protect companies during the research and design phase of product development (Goldstein, 2007).

Types of Information

There are many types of information that is sought after by criminals engaging in economic espionage. When referring to information, it is important to understand that not only is organized data sought after, but any piece of information that could impact an organization if it becomes compromised by the wrong individual (Winkler, 1997). For example, even source code can be considered a trade secret as long as it is classified as a trade secret and derive independent economic value which was decided in USA v. Aleynikov. As stated previously, information can come in many different forms and varieties.

Information sought after by criminals can be technologically sophisticated to simple forms of paper, and even trash (Sepura, 1998; Winkler, 1997). First, technology based information is the most common form in which information is stored. Specifically related to computer based information is e-mail (Coskun & Jacobs, 2003). E-mail creates great risks for companies; most people using it do not think about how they are using it. This technological advancement is used to transmit all types of corporate information and is easily accessible by white collar criminals. Simple computer hacking (i.e. accessing the e-mail server), or just observing an open e-mail (or a paper print out of the message) on an unattended computer can have devastating effects to organizations. Second are formal documents that are used by companies for a variety of purposes (Winkler, 1997). These must all be printed out and kept as hard-copy documents, stored most commonly in file cabinets. Third are draft documents, which are often referred to as "worthless" (Sepura, 1998; Winkler, 1997). Most people assume that once the final product is produced, draft documents hold no value. The information these documents contain can be highly valuable. Fourth are working papers, the precursors to formal documents. Again, these documents are often thought of as not valuable, but they often contain information and specifications of outlining projects (Coskun & Jacobs, 2003). Fifth are scrap papers, which are almost always thought of as invaluable. Scrap paper often contains parts of the final project on different pieces of scrap (Coskun & Jacobs, 2003). If a criminal can collect scrap, he/she may be able to put together the pieces of the whole to gain information and harm the company.

Next is the legal and formal aspects of running a business. Internal correspondence, legal and regulatory filings, other records, and the media are all types of information that corporations use to spread information. Internal correspondence contains a substantial amount of information

pertaining to a company's intellectual property (Winkler, 1997; Coskun & Jacobs, 2003). Internal correspondence is used to share information within an organization through the use of newsletters, policy documents, or meeting minutes (Coskun & Jacobs, 2003; Fraumann, 1997). This spread often contains highly sought after information in order to keep employees informed on company growth, such as legal and regulatory filings.

Legal and regulatory filings, are documents that companies are legally required to produce (Winkler, 1997). These filings and documents are often revealing to companies trade secrets and become accessible by anyone under the Freedom of Information Act (FOIA). Other records, such as hotel, airline, and car rentals, are highly sought after by economic espionage spies. These records help the spies track targets and plant tracking or eavesdropping devices to follow and record possible confidential business transactions (Winkler, 1997). Almost anything anyone does in today's technologically advanced world creates a record that can create vulnerabilities for companies.

Also important in the theft of trade secrets is media or open source information. This is anything that is publically available for viewing or direct access. In other words, this is a form of competitive intelligence, the process of legally gathering information to understand the competition within the global market (Crane, 2005; Slate, 2009). Without the use of competitive intelligence, companies would easily become obsolete.

Another type of information is corporate communication. There are three main types of corporate communication: formal meetings, informal meetings, and casual conversations (Winkler, 1997). Formal meetings often contain the most sensitive information regarding intellectual property. These meetings often include the highest officials within an organization and discussions of future plans and developments. Informal meetings are anytime employees get

together to talk about work either in person, over the telephone, or a gathering in a common area (Winkler, 1997). The information discussed in these informal meetings ranges greatly and can include sensitive corporate information. Lastly, and the most overlooked, is casual conversations. These types of conversations usually take place in open, public places where there is no expectation of privacy, as is the case with the other two types of communication (Winkler, 1997).

These classifications of information are important in understanding how criminals access sensitive information. As identified by the literature, the most common ways in which sensitive material is accessed are from the types of information that are deemed the least important by both the corporation and its employees (Winkler, 1997). These types of information can be e-mail, casual conversations, and/or scrap paper. These are often the easiest for criminals to access because they are the most common forms of business transactions (Winkler, 1997; Fraumann, 1997; Coskun & Jacobs, 2003). Even though the three types of information are often overlooked as valuable, it is important for a company to work to protect all types of information (Winkler, 1997). In order to reduce the likelihood that a company, organization, or individual may become victimized, there needs to be the use of risk evaluation.

Risk Evaluation of Economic Espionage

In order for economic espionage to occur, there must be risk. "Risk is the driving consideration of all corporate espionage activities" (Winkler, 1997, p. 12). Risk is defined by the probability that company (or a person, in some cases) will become a victim of an undesirable event (Baker & Benny, 2012). In this context, there are several types of risk that an organization needs to consider. These risks can be organizational and/or reputational (Minott, 2011; Schanz, 2006). Organizational risk is what the organization stands to lose from the theft.

Reputational risk is how the company's stakeholders and investors will be affected by the theft. For example, the trust that the company has with its investors will be tested if an occurrence of economic espionage is identified. Winkler (1997) identifies an equation that can be used to estimate the amount of risk a company can expect. The formula for the risk equation is displayed in figure 1.1.

Figure 1.1. **Risk Equation** (Winkler, 1997).

$$\text{RISK} = \frac{\text{THREAT} \times \text{VULNERABILITY}}{\text{COUNTERMEASURES}} \times \text{VALUE}$$

The risk equation (Figure 1.1.) includes four essential components: value, threat, vulnerability, and countermeasures (Winkler, 1997). Value refers to the worth of the desired information. This can be monetary or the stake it has in the global market (Winkler, 1997). In conjunction with both monetary and global market control, a company's reputation is also at risk (Minott, 2011). A threat is anyone or anything that is willing and able to access your information. One of the biggest threats to any organization, industrial spies, also use their own version of the risk equation when deciding whether or not to engage in economic espionage (Schwartau, 1994). Human or natural vulnerability refers to weaknesses within an organization that makes it easier for white collar criminals to engage in economic espionage (Baker & Benny, 2012). Vulnerabilities can be categorized as any weaknesses in an organization's security functions (Baker & Benny, 2012). Countermeasures, meanwhile, (discussed later in this study), are anything an organization or individual does to create an environment that is difficult to penetrate in order to access intellectual property (Winkler, 1997).

These four components of the risk equation are important to understand (Winkler, 1997). These components allow for an effective and appropriate plan to be structured into a corporate environment to help safeguard intellectual property. Once a company or an individual can successfully identify these four components, it can successfully begin to limit the amount of risk involved within the organization (Winkler, 1997; Baker & Benny, 2012).

Threats evaluate the risk involved in engaging in economic espionage in the context of the probability of detection. Most of the time there is little risk involved for the spies; therefore, the occurrences of attempting to steal intellectual property is high (Winkler, 1997). Garcia (2005) expands on this type of calculation in explaining the probability of detection. The probability of detection is based on multiple factors. These factors can include physical security measures and software programs to detect unauthorized intrusions into a corporations private computer network (Garcia, 2005). Ultimately, the longer the time delay between the criminal act and the actual detection, the less likely it is for a criminal to get caught. Another calculation that spies make is one regarding the detection potential (Baker & Benny, 2012). Spies often use a rational hedonistic calculus; that is, they calculate the costs of detection against the possible benefits of obtaining the intellectual property (Gibbs, Cassidy, & Rivers, 2013). The literature, however, identifies that most companies do not have the proper countermeasures in place. Therefore, the risk for spies is relatively low, while the occurrence of economic espionage is high (Minott, 2011). Even if companies or individuals practice proper countermeasures, they will never be totally risk free. Once the risk calculation is complete, the intelligence process begins.

The intelligence process is the gathering of information about organizations and individuals (Pellissier & Nenzhelele, 2013). The intelligence process has four phases: definition

of requirements, collection, analysis, and evaluation. The intelligence process is circular in nature and dynamic. For example, as information is gathered, it may result in new requirements (Winkler, 1997).

Defining requirements is essential to any good espionage operation. In other words, if spies know exactly for what they are looking (the defining requirement), they will be better able to find the required information (Winkler, 1997). Once the requirements of the operation are defined, the collection process begins. The collection process satisfies the outlined requirements (Winkler, 1997; Pellissier & Nenzhelele, 2013). That is, the collection process identifies and plans out how the desired information will be acquired. Sometimes the information is readily available to the spies or a more in-depth process must be used. An important countermeasure to the collection process is disinformation: the process of misleading spies by displaying falsified information (Alexander & Smith, 2011). For example, an organization may change the name of a file to make it appear as desirable, but once stolen, the criminal may not have the information he/she was after.

Once the information has been collected, the receiving organization or individual begins the analysis phase (Pellissier & Nenzhelele, 2013). There are two different types of analysis: standard and traffic. Standard analysis is the examination of the actual data collected, while traffic analysis is the examination of data flow (Winkler, 1997). For example, traffic analysis would be conducted while information is being collected, while the criminal is searching for what he/she desires. Standard analysis would be conducted on the acquired information to understand how to use it to gain a competitive edge.

Lastly, is the evaluation process. The evaluation process is determining how well the information collected meets the defined requirements of the information process (Winkler, 1997;

Pellissier & Nenzhelele, 2013). In other words, the criminal entity is evaluating the information in order to see if it meets the desired specifications. During the evaluation process, the criminal, identifies whether or not the illegally acquired information is what is needed in order to gain a profit.

A company can reduce its risk by following the risk equation and engaging in proactive risk management activities (Crawford & Strasser, 2008). Risk management is techniques used to reduce the risk associated with daily business functions. As business functions are dynamic, the risk management process must continually change to be best suited to protect company assets. If the risk is still high, a company can create more physical and non-physical (i.e. technological) countermeasures (Crawford & Strasser, 2008). If a spy's risk calculation is low, he/she will engage in economic espionage by engaging in the information process (Winkler, 1997). For example, if the spy calculates that there is little risk of getting caught, he/she will begin the necessary process to engage in economic espionage. The information risk management process is dynamic and always adapting to the information collected by spies worldwide. With new technologies and new areas of market dominance, spies and criminals alike must adapt to identify the most valuable information to steal.

Threats

A threat is defined as a person, organization, event, or condition that could hurt a company in an undesirable manner, either man made or natural (Baker & Benny, 2012; Winkler, 1997). A man made threat can be an employee. A natural threat can be things such as a floor or tornado, which may destroy buildings allowing direct access to sensitive information. Whenever a company or individual holds information that could possibly have value to someone or something else, the threat of economic espionage still exists (Winkler, 1997). Most threats are

direct in nature, but they can also be indirect. For example, a company could possess information about another targeted company, which in turn makes the first company a secondary target (Winkler, 1997). If two companies are working together to develop a new product, and one is a target, the other also becomes a target through association.

The largest and most common threats to any organization can be classified under the two broad categories of either human/man-made or natural. Organizations are vulnerable to theft by human adversaries. These human adversaries can be subdivided into internal and external adversaries. Most importantly is that the loss of information can be unrecoverable and completely destroy a company (Winkler, 1997; Minott, 2011). Threats can be internal employees, competitors, foreign competitors, and domestic competitors (Sepura, 1998). As such, perils can damage reputation and lead to a loss of economic dominance, loss of stakeholders, and ultimately a loss of substantial income (Minott, 2011).

Man-made & natural threats. There are also different types of perils – the individual who leads to the threat. That is, the human adversary is responsible for the theft of valuable information. Human adversaries, meanwhile, can be classified into the broad categories of internal and external (Sepura, 1998). Internal adversaries are specific to the employees of that organization or company (Vashisth & Kumar, 2013). These can be both current and former employees, and they are often very difficult to identify because companies often fail to recognize that a "trusted employee" may actually engage in a variety of nefarious actions that could expose the company to a variety of risks (Vashisth & Kumar, 2013). In fact, a typical internal spy may appear to be one of the hardest workers. A worker who does his/her job to a high level often never gets questioned or observed in-depth, making it easy for him/her to slip away with valuable information (Winkler, 1997).

Explanation. There are many reasons why internal employees may commit economic espionage, such as because they are: disgruntled, thrill seeking, or departing (Winkler, 1997). Another major factor is the financial aspect (Sepura, 1998). Individuals may engage in economic espionage to display how profitable a simple criminal act can be. Former employees may engage in economic espionage out of vindictiveness, to receive a payoff, or to impress a new boss.

Lastly, on-site non-employees, ideologues, and activists also pose a threat to companies. (Winkler, 1997; Sepura, 1998). In other cases, internal threats may be compromised in some manner. For instance, a common "Cold War" tactic was to place an employee in a compromising situation and then blackmail that individual for specific information. If nor extortion, in other cases, trusted employees are actually "tricked" by individuals where they inadvertently or purposefully provide an individual company secrets out of devotion or love (Schweizer, 1993).

Competition. In other cases, competitors themselves engage in corporate espionage. Externally, competitors pose the biggest threat to companies' worldwide. A competitor is any business that seeks to gain control of the global market at the demise of another entity (Sepura, 1998). Midsize companies face the largest competition and are less aware of possible threats because most hold the mentality that they are not large enough to be victimized or the information they possess has no intrinsic value (Winkler, 1997). More specific to the United States are its foreign competitors. The threat from foreign competitors is often complex (Winkler, 1997; Sepura, 1998; Everest-Phillips, 2007; Fraumann, 1997; Slate, 2009; Pacini et al., 2008). For example, "multinational corporations know exactly what they can and cannot get away with, and they become experts at covering their tracks" (Winkler, 1997, p. 53). Another example, multinational corporations know the nature and extent of the law and understand what

is legal or illegal. If the action they desire to pursue is illegal, these corporations use techniques that are hard to detect and have the resources (financial stability) for an expert legal team to help protect them from legal prosecution (Crane, 2005).

Foreign Nations. More than 100 nations worldwide target the United States to carry out their acts of economic espionage (Fraumann, 1997; Pacini et al., 2008). Many of the operations carried out against the United States are government funded, and the individuals are never held legally responsible, giving foreign nations a sense of immunity (Winkler, 1997; Sepura, 1998). Most existing laws, for example, only protect domestic intellectual property, therefore, when economic espionage is committed internationally, it is not considered a crime (Sepura, 1998). Secondly, when a different state is victimized, they hardly every take punitive action. For example, when the United States were alerted of French spies being within the corporation of IBM, the United States responded by simply sending a letter of diplomatic protest (Sepura, 1998). It is occurrences like these that do not create general deterrence and promote the continuation of economic espionage. Both hostile and allied nations are among many which target the United States for intellectual property (Pacini et al., 2008; Fraumann, 1997).

Hostile Nations. Hostile nations are less concerned with political embarrassment when engaging in economic espionage against the United States. Without the fear of getting caught, these nations are far more likely to commit economic espionage than their allied counterparts (Winkler, 1997; Sepura, 1998). These nations are willing to take more risks and use more aggressive, overt tactics. These hostile nations realize now that economic prosperity is more important than military intelligence, and are therefore making economic espionage an important part of their strategic plan (Fraumann, 1997). The hostile nations are identified as: Russia, China, Iran, and Cuba (Coskun & Jacobs, 2003; Fraumann, 1997; Slate, 2005; Winkler, 1997). It

is outstanding what these countries can do to companies in the US. For instance, a more obvious and well known tactic used by the former USSR was the installment of the KBG in foreign Nations worldwide to gain access to intellectual property (Winkler, 1997; Fraumann, 1997). In a more covert manner, China employs intrusive measures through the use of visiting students and professors (Fraumann, 1997). They use these students and professors to infiltrate corporate and academic laboratories and send their findings back to the Chinese government (Sepura, 1998).

Allied Nations. The United States' allies are some of its greatest competitors not only in the global market, but also within the American economy (Winkler, 1997; Fraumann, 1997). Nearly all of the nations considered to be United States' allies target the United States for intellectual property. Of the many allied nations that target the United States, there are a few that do it on a regular, more extreme basis. These nations are: Japan, France, Israel, and Germany (Winkler, 1997). Schweizer (1993), in his book *Friendly Spies*, reveals that many counties which have been military allies of the United States are in fact at "war" with the United States economically. These countries include England, France, Germany and Israel. For example, France "bugged" first-class cabins of Air-France planes to record the conversations of international businessmen, allowing them to monitor the conversations of high class corporate executives (Schweizer, 1993). While Schweizer (1993) provided many case studies of these "Friendly Spies" since his publication, other authors have identified additional "Friendly Spies" from nations such as Japan and South Korea (Fraumann, 1997). In these cases, the country itself might engage in espionage using the resources of the nation, or the state may employ agents to target certain companies and even universities to steal intellectual information that can be later used in the military and economic development of that particular country (Fraumann, 1997; Sepura, 1998).

Organized Crime. Organized crime groups can be found throughout both the United States and worldwide (Winkler, 1997). . Some of the most popular organized crime groups can be identified as the Italian Mafia, the Eastern Bloc mafias, and drug cartels. Organized crime groups most often pose a minimal threat but still have damaging capabilities. Most often, organized crime groups are often found involved in economic espionage when their services are contracted by an organization to steal from its competitors (Winkler, 1997). The most common techniques that these organized crime groups use are computer hacking and misrouted transactions (Winkler, 1997). For example, Russian crime rings have stolen $1 billion from the United States over hacked computer networks (Fraumann, 1997; Maxwell, 1998).

Petty Crime & Hackers. There are other smaller, less organized forms of threats that organizations and individuals should be made aware (Winkler, 1997). First and foremost is petty crime. The criminal, for example, may steal a personal computer and unknowingly have also stolen intellectual property that could be valued much higher than the personal computer itself (Winkler, 1997). More specifically, in 1997, a thief targeted Levi Strauss & Co. and managed to steal a computer hard-drive from the company. On this hard-drive were the names, birthdates, and social security numbers of thousands of employees (Machlis, 1997). A more recent example, during the period 2006 to 2012, the Western District of Pennsylvania indicted a group of five Chinese nationals who had either conspired to or actually hacked into United States' companies in order to benefit Chinese competitors (Department of Justice, 2014). This group of individuals each planned to hack into American entities and maintain access to their computer networks in order to steal information.

Secondly, hackers also pose a threat to any organization. Hackers are individuals who have an in-depth understanding of the internet and how the internet functions (Barber, 2001b).

The fear that hackers present to organizations gives hackers the persona that they are unstoppable (Barber, 2001a.). However, most hackers are simply curious and want to explore and discover things on the internet; they like to test their individual skills to see if they are capable of breaking into protected systems (Barber, 2001b). Hackers will often exploit vulnerabilities that cannot be fixed. A hacker will be able to break through a computer firewall because the software unknowingly has a weak point that cannot be fixed (Winkler, 1997). For example, a skilled hacker can write code and run applications; these are most common to be continuous and automated (Barber, 2001a.). One of the biggest motivations for hackers is, in fact, economic espionage (Barber, 2001b). Hackers often gain access to an organization's system without company knowledge and do so for an extended period of time. Once the desired information is obtained, hackers are able to remove all traceable evidence, making it difficult for hackers to be caught and criminally prosecuted. Hackers are constantly evolving and perfecting their abilities, which contributes to their effectiveness and makes them hard to detect (Barber, 2001a).

In today's advanced technological society, there are numerous threats that will continue to occur without recognition. All nations, both hostile and allied, target the United States for the vast intellectual property its organizations hold (Fraumann, 1997; Schweizer, 1993). Often times, organized crime groups do not pose a large threat unless they are contracted by another organization to steal from competitors (Winkler, 1997). Lastly, hackers and petty crime pose a minimal threat, unless by chance, the individual unknowingly comes across intellectual property.

Vulnerabilities

Once threats have been identified, an organization must understand its vulnerabilities in order to better safeguard its intellectual property (Winkler, 1997). Vulnerabilities are the weaknesses in an organization's security functions (Baker and Benny, 2012). The fewer

vulnerabilities a company contains, the less likely it is to have risk. The best way to succeed at reducing risk is to understand organizational weaknesses, and how criminals access valuable information (Winkler, 1997; Baker and Benny, 2012). Organizations face operational, physical, personnel, and technical vulnerabilities (Winkler, 1997).

Operational vulnerabilities are weakness that result from an organization's daily tasks (Baker and Benny, 2012). These are most likely to precede an occurrence of economic espionage (Winkler, 1997). Operational vulnerabilities are: poor awareness of preexisting security operations, social engineering, accidents and carelessness, poorly developed policies and procedures, predictability, failure to act on sound procedures, detailed sales and marketing, public relations, and lastly, giving out too little information. Social engineering for example, is when a person acts as if he/she is in a trusted position in order to receive passwords from employees. Predictability refers to a company's routine, and doing the same action in a repetitive manner. Detailed sales and marketing affects a company when they release too much information about an upcoming and newly developed product. Lastly, giving out too little information can create vulnerabilities for a company by giving the appearance that the company may be hiding something valuable. These operational vulnerabilities, coupled with physical vulnerabilities, make it difficult for a company to safeguard its assets (Winkler, 1997).

When physical security comes to mind, most individuals think of uniformed patrol officers, fenced property, electronic locking doors, and heavy iron doors that seem to be impenetrable (Winkler, 1997). However, physical security is defined as, physical measures "designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them from: espionage, sabotage, damage and theft" (Baker & Benny, 2012, p. 1). With the criminal act of economic espionage, the physical security

component to protecting one's assets is much more in depth and includes many components that are often overlooked (Winkler, 1997). Physical vulnerabilities related to economic espionage include, but are not limited to: poorly informed guards, lacking access controls, garbage (i.e., not shredding valuable materials), open storage (i.e., not locking file cabinets), information storage (i.e. password protected computers and logins), copy machines (i.e., leaving copied information on the printer), neighbors (i.e., eavesdropping), loss of control due to natural disaster, smaller equipment style (i.e., smaller equipment is easier to conceal and steal), no regularly scheduled audits, messy desks (i.e., hard to notice when important things go missing), leaving valuable information in mail boxes, not logging off computers, lack of the use of available locking equipment, power failure, and placement of building and equipment (i.e., a computer by an open window is easier to steal). In collaboration with physical and operational vulnerabilities, an organization must also consider personnel vulnerabilities and technical vulnerabilities (Winkler, 1997)

Personnel vulnerabilities are similar to operational vulnerabilities. Personnel vulnerabilities are "related to the ways in which companies hire and manage their employees" (Winkler, 1997, p. 121). These can include, but are not limited to: failure to validate claimed backgrounds, susceptibility to criminal behavior, and isolation of human resources and personal hardships (Winkler, 1997).

Technical vulnerabilities are related to an organization being victimized without having to be on the premise (Fraumann, 1997). Technical vulnerabilities can include: configuration errors, which leave unintentional access points for criminals; poor password creations; difficult to detect system modifications (i.e. the more complex the system, the harder it becomes to detect changes); easily accessible modem; poor data storage; data transmission across computer

networks' virtual computer access (i.e. accessing computers from hundreds of miles away); electromagnetic pulse; wire taps; and bugs (i.e. small electronic recording devices) (Fraumann, 1997).

With so many vulnerabilities of which companies have to be aware, it is virtually impossible for a company to be impenetrable (Winkler, 1997). Not only do companies have to be concerned with internal vulnerabilities, but they must be aware of vulnerabilities that may go undetected. Undetected vulnerabilities are the most damaging to companies worldwide (Winkler, 1997). Company risk, combined with a high amount of vulnerabilities, leads to the occurrence of economic espionage; therefore, a company or entity must institute counter measures (Winkler, 1997; Hemphill, 2013).

Occurrence of Economic Espionage

Although this is not always the case due to a company's reputational risk, once a company feels that it has been a victim of economic espionage or theft of trade secrets, the company may report it to any law enforcement agency (Desmet, 1999). Once the complaint is made, the US Department of Justice, in particular, the Federal Bureau of Investigation, may become involved. This federal agency, along with Department of Justice, is responsible for arresting and prosecuting the individual, or individuals, responsible for this criminal act (Desmet, 1999). Although this process seems relatively simple, companies may be hesitant to bring about a criminal conviction due to the discovery process and their reputation.

There are many reasons for not reporting. The most common reasons are negative publicity, embarrassment, the threat of losing future investors, shareholder frustration, and further exposure of other trade secrets during the prosecution process (Desmet, 1999). For these reasons, the true extent of the worldwide problem of economic espionage and trade secret theft is

hard to determine. These crimes are often difficult to assess due to the "dark figure of crime," which is unreported crimes to criminal justice officials (Minott, 2011). Although the problem is often underreported, there are several factors that have led to this steady increase in occurrence.

One of the major contributing factors is due to the insurmountable pressure for economic dominance. Many organizations, and even nation states, resort to economic espionage in order to maintain a competitive level within the world market. (Coskun & Jacobs, 2003). Because of this pressure to gain economic dominance, companies have moved away from leadership, concerns with resources, and productions costs (Coskun & Jacobs, 2003). Companies who are in need of gaining economic dominance may engage in criminal activities rather than ethical means. Now, the goal of corporations is to dominate the world market at all costs and have a strong emphasis on management and market composition (Coskun & Jacobs, 2003). Secondly, companies who lack the resources necessary to generate corporate intellectual capital engage in economic espionage or trade secret theft in order to compete in the competitive world market (Coskun & Jacobs, 2003). In fact, it is just as important to generate corporate intellectual capital as it is to be the first company to market a new product (Coskun & Jacobs, 2003). Smaller, less sophisticated companies do not have the time and resources available to generate intellectual capital; therefore, they are more likely to engage in economic espionage or trade secret theft (Coskun & Jacobs, 2003). Lastly, the lack of protection and globalization make intellectual property easily accessible to competing companies (Coskun & Jacobs, 2003). Because of the increase in occurrence of economic espionage, legislators created laws to try to combat and deter the commission of economic espionage.

Previous Legislation Combating Economic Espionage

Before the discussion of the Economic Espionage Act of 1996, it is important to understand and discuss the evolution of economic espionage related laws in the United States. These laws are developmental in nature. Previously, companies' trade secrets were classified as property rights (Desmet, 1999). Traditionally, prosecutions involving the theft of trade secrets were tried under tort violations in civil court (Desmet, 1999). In particular, there were the protections of patents, copyrights, trademarks, and trade secrets. At the state level, there is the Uniform Trade Secrets Act, the National Stolen Property Act, the World Trade Organization, and the Trade-Related Aspects of Intellectual Property Rights Agreement. At the federal level, different attempts have been made to help companies protect their valuable assets. The National Stolen Property Act of 1948 was among the forefront of federal statutes to combat trade secret theft (Desmet, 1999).

The National Stolen Property Act, which was enacted by the United States in 1948, "prohibits the transportation, transmission, or transfer of any goods, wares, merchandise, securities, or money of the value greater than $5,000, knowing the same to have been stolen, converted, or taken by fraud" (Desmet, 1999, p. 104). Due to the narrow scope of the law, trade secret theft prosecutions were unsuccessful (Desmet, 1999). This was because the law was initially directed at property crime, not intangible property such as trade secrets.

Stemming from the World Trade Organization, the Trade-Related Aspects of Intellectual Property Rights Agreement provided members of the World Trade Organization dispute resolution (Effron, 2003). Civil suits were also often used to gain compensation from losses, but

these were not applicable to all victims (Desmet, 1999). For example, small businesses might spend more in legal fees in comparison to the value of their financial losses (Desmet, 1999). With all of these failed attempts to combat and deter individuals from engaging in economic espionage and theft of trade secrets, major legislative reform was necessary to enhance the effectiveness of prosecution.

In 1979, the Uniform Trade Secrets Act was enacted to create the first attempt at an all-inclusive legislation to combat trade secret theft (Desmet, 1999). The Uniform Trade Secrets Act (UTSA) allows a party to sue and recover stolen assets from a third party, both civilly or criminally (Desmet, 1999). Criminal prosecutions can result from theft of misappropriation of trade secrets. The victimized company can attempt to criminally prosecute the offender, and if it feels as though it did not receive enough compensation, the victimized company can file a civil lawsuit.

A total of 42 states have attempted to enact state laws modeled after the Uniform Trade Secrets Act, but they have shown to be unsuccessful due to the lack of resources needed at the state level (Desmet, 1999; Goldstein, 2007). In combination with the lack of resources, lack of uniformity creates confusion as to what economic espionage is and how it should be tried at the state level (Desmet, 1999). Therefore, the Economic Espionage Act (EEA) of 1996 was created as a federal law to help companies protect their intellectual property.

The Economic Espionage Act of 1996

The Economic Espionage Act (EEA) of 1996 was signed into law by President Bill Clinton on October 11, 1996. EEA was created to criminalize the theft of trade secrets and increase the likelihood of preservation of investments. The major goal of the EEA was to

maintain fair market competition and prevent corporate spies from stealing from their competitors (Desmet, 1999).

The Economic Espionage Act of 1996 gave way to a more specific definition of the term "trade secret" (Effron, 2003). The act created two new federal crimes with respect to theft of trade secrets (Edelman, 2011). These laws are cited under section 1831 and 1832 of the EEA. The EEA consists of eight subsections, §1831-1839, prosecuting cases of economic espionage under section 1831 and 1832. Table 1.1 displays a brief overview of the entire act. A full representation of the Economic Espionage Act of 1996 can be found in Appendix A.

Figure 1.2. **The Economic Espionage Act of 1996**

Sub Sections	**Explanation**
§1831	**Economic Espionage**- Used to prosecute foreign nations
§1832	**Theft of Trade Secrets**- Used to prosecute individuals
§1833	**Exceptions to Prohibitions**- Used to protect legal activities such as competitive intelligence
§1834	**Criminal Forfeiture**- Requires any and all information acquired during the criminal act be returned to the United States
§1835	**Orders to Preserve Confidentiality**- The court shall protect and preserve the trade secrets that are being discussed during trial
§1836	**Civil Proceedings to Enjoin Violations**- The district courts hold exclusive jurisdiction for civil actions
§1837	**Applicability to Conduct Outside the United States**- Applies to those who are natural person or citizen of the United States
§1838	**Construction with Other Laws**- The law must work in conjunction with other remedies
§1839	**Definitions**- Defines all vague terminology within the act

Section 1831

Section 1831 is directed against foreign countries. It provides more severe penalties if the offender had intent to benefit a foreign government, foreign company, or foreign agent by stealing trade secrets (Edelman, 2011). In order for the government to have a successful conviction under section 1831, it has to prove three items. First, the government must prove the defendant, "knowingly possessed, received, or bought a trade secret" (Edelman, 2011, p. 457). Secondly, the government must prove that the defendant knew the trade secret was obtained illegally. Lastly, the government must prove the defendant intended or knew that the theft of trade secrets would benefit a foreign entity. (Edelman, 2011).

Section 1832

Section 1832, Theft of Trade Secrets, is the more general of the first two sections (Edelman, 2011). Section 1832, "makes it illegal for a person to, among other things, possess a stolen trade secret with the intent to convert that trade secret to the economic benefit of anyone other than the owner thereof" (Edelman, 2011, p. 457). There are three elements of intent required under section 1832. First, "the defendant must knowingly commit one of the listed acts of misappropriation" (Desmet, 1999, p. 112). Next, "the defendant must act with intent to convert a trade secret to economic benefit of anyone other than the owner thereof." Finally, "the defendant must act with the intentions of knowing the offense will injure any owner of that trade secret," (Desmet, 1999, p. 112). The penalties associated with section 1832 vary depending on mitigating and aggravating circumstances (Desmet, 1999). None the less, penalties for benefiting a foreign entity are much more severe than committing one for a personal gain (Desmet, 1999).

Penalty Enhancement

In an effort to increase deterrence and reduce the amount of theft that companies of the United States face each year, congress imposed the Foreign and Economic Espionage Penalty Enhancement Act of 2012on January 14, 2013.This act increased the maximum fines for foreign and economic espionage to not more than $5 million for individuals and not more than $10 million or 3 times the value of the stolen trade secret. This law also allows for review by the United States Sentencing Commission. The sentencing commission can review, and if applicable, change the sentencing guidelines and policy in order for the punishment to be more suitable for those persons convicted of offenses relating to economic espionage. A full representation of the Foreign and Economic Espionage Penalty Enhancement Act of 2012 can be found in Appendix B.

Countermeasures

Protecting a company against economic espionage, or the theft of trade secrets, is not a simple task. In fact, it is possibly the most difficult task a company faces (Winkler, 1997). Trade secrets are loosely protected by both state and federal laws and can be expensive for companies to protect their valuable assets (Ronde, 2001). Simple and relatively inexpensive measures to help combat the occurrences are as follows.

Pacini et al. (2008) identify four factors to be considered when implementing protection measures: size of company, risks within the business, history of security problems, and industry and/or government standards. The first step is to identify company information that would be valuable to competing companies and keep this information confidential (Pacini et al., 2008). Hannah (2005) identifies two types of protection procedures commonly used in corporations. The first is the use of access restriction, which restricts certain areas and prohibits employees

from entering these areas. The second method is handling procedures, which state what employees can and cannot do when in contact with company trade secrets. These employee restrictions should be present in protection measures to help contain the spread of information by employees (Pacini et al., 2008). Employees who understand company policies and guidelines help safeguard against victimization by understanding what is allowed and the possible sanctions for misappropriating information (Hemphill, 2010). Lastly, Pushkar (2005) identifies employment agreements. These consist of the employee reading guidelines and restrictions, which limit access and movement of intellectual property. Employees should then sign a document stating that they have read and understand policies and procedures and will not misappropriate valuable information (Pushkar, 2005). Covenants, which are employee signed agreements not to disclose information received on the job, are also used as an attempt to keep employees loyal to their company during and after employment (Pushkar, 2005; Goldstein, 2007).

Winkler (1997) expands on these techniques and gives a detailed explanation of steps companies should take in order to reduce the risk associated with competing in a global market. Organizations should create awareness training programs, classify valuable information, install security alert systems, offer reward programs, require sensitive information to be transmitted on a face-to-face basis, verify access to rooms and computer networks, and verify identity of employees. Employee badges should have no personal identifiers, and employees should sign agreements, releases, and be briefed on how to handle sales representatives and suspicious activity. Employees should not use cellular phones, and conversations outside of work should not include company information. Employees should alter daily work routines, include security in business meetings, involve security in policy updates, implement clear and sound disaster and

incident procedures, and conduct penetration testing. Corporations should conduct background checks on employees, check spouses and immediate family of employees, offer an anonymous employee hotline, maintain open lines of communication between departments, conduct audits, monitor visitors, classify employees, implement the use of locks and password protect electronic data, and remove clutter from the workplace. Corporations should also encourage the use of security reminders, shredders, locked trash containers, access control, anti-virus software, computer systems backups, multiple firewalls, bug and wiretap sweeps, and the use of encrypted data during transmission (Winkler, 1997).

It should be noted that these safeguards are not fully effective, and the threat of being victimized still exists even with these precautions. By implementing these recommendations in part or in whole, the risk of victimization may be reduced (Hannah, 2005; Pacini et al., 2008; Pushkar, 2005; Ronde, 2001; Winkler, 1997). In fact, companies who take the proper steps to reduce vulnerabilities, will have less risk, in turn making that organization less desirable to criminals of white collar crime (Winkler, 1997).

Research on Economic Espionage, Theft of Trade Secrets, and Intellectual Property Theft

The research relating to economic espionage is relatively informative; however, it is limited. This research can generally be divided into three common areas: early industrial anecdotal stories, pre-EEA research, and post EEA studies. During the 1960s, concerns of economic espionage in advancing technological industries and the need for better protection of assets were among the forefront of research (Hamilton, 1967). As time progressed, research began to focus on specific cases of economic espionage, theft of trade secrets, and the specifics pertaining to victimization and offender status.

Historical case studies. The use of spies to steal intelligence from competitors is not a new phenomenon; it began with the development of the global market and international trade and can be found all throughout history (Bergier, 1975). For example, Bergier writes that as early as mid-6th century AD, a princess traveled to China and placed silk worms in her flowered hat. She then brought them back to Europe in order to understand how silk was produced. Another early secret before the industrialization of society was how to master flints. The Cretans held this technology and spies were sent to gain knowledge on this delicate process. It was not until the industrial revolution that the involvement in trade secret theft offered more than just knowledge on how to produce goods.

During the 18th and 19th century and the industrial revolution, China was the first nation to discover and mass produce porcelain (Bergier, 1975). Because of porcelain's potential for wealth, many nations sent spies to steal the manufacturing process from China. France was the first successful nation in doing so. From that point forward, many nations were also successful in gaining access to the manufacturing process of porcelain. Other highly sought after information included: rocket technology, hermetic sealing, gunpowder, acids, food preservation, the manufacturing of gold, antimony, steel, cold light, and purification of diamonds (Bergier, 1975).

From the late 1800s through the early 1900s, military espionage began to move to the forefront. This military intelligence was centered on technologies that could help countries win war battles (Bergier, 1975). Specifically during World War I and World War II, spies were relied on heavily to gain a military advantage. The most highly sought after information during this time period was: poison gas, explosive missiles, ammunition technologies, submarine technologies, rust proof steel, cannons, and atom bomb technologies. Although war technologies

proved vital to spies during war times, once the war came to an end, the return to industrial espionage took place (Bergier, 1975).

Theft of intellectual property. Most research does not examine economic espionage per say, but rather the theft of intellectual property which is highly relevant to the EEA. For example, Almeling et al., (2010) analyzed federal civil court cases between 1950 and 2008 to grasp a better understanding of litigations. Almeling et al. (2010) found that in over 85% of all cases analyzed, the offender was someone whom the owner of the trade secret knew. The authors also found that in nearly 42% of the cases analyzed, the owners of the trade secrets prevailed in the decision of the trial.

Criminal acts of economic espionage have a variety of effects. Andrijcic and Horowitz (2006) found that attacks that have a longer lasting effect create more harm than that of short term effects. For example, Andrijcic and Horowitz found that numerous small attacks which produce small profits are less effective than one large attack. They argued that the theft of a trade secret will result in long term loss, potentially hindering the company of a large sum of possible income. Andrijcic and Horowitz (2006) found that the most likely targets of economic espionage are computer and electronic product manufacturers; motor vehicle, body, trailer, and parts manufacturers; chemical manufacturers; machinery manufacturers; fabricated metal products manufacturers; publishing including software; plastics and rubber products manufacturers; primary metal manufacturers; nonmetallic mineral products manufacturers; and wood products manufacturers. Andrijcic and Horowitz (2006) found that of these ten sectors, chemical manufacturers are the most victimized because these companies hold the greatest market value and have the largest number of competitors (Andrijcic & Horowitz, 2006). At the highest risk of victimization are electronics, motor vehicles, machinery, and chemical

manufacturers (Andrijcic & Horowitz, 2006). It is important to note that not any one company is totally safeguarded from economic espionage (Andrijcic & Horowitz, 2006). Any time a company has competition, holds a great deal of the economic market, or has the ability to change the global market, that company is at risk of being victimized. Therefore, because of the constant pressure to be the leader in the global market, essentially all companies involved in daily business routines are susceptible to economic espionage (Coskun & Jacobs, 2003).

Contemporary Case Studies. In modern society, economic espionage is considered to be class two information warfare (Schwartau, 1994). Class two information warfare is related to how the stolen information is used, rather than how the information was acquired. Economic espionage is focused on how companies can gain a competitive advantage in large economic spheres rather than just gaining an advantage over one single competitor. Class one warfare, meanwhile, refers to attacks on an individual's electronic privacy (Schwartau, 1994). The following examples will demonstrate how foreign competitors used economic espionage to gain a competitive advantage.

China is one of the most common nations that engages in economic espionage. The Chinese have constructed corporate competitive intelligence programs to help China collect and steal intellectual property from the United States and other nations holding valuable information (Slate, 2009). Slate (2009) found that the Chinese are experts at what they do. For instance, they have been known to be the world's leading product counterfeiters for over 300 years (Slate, 2009). As China seeks to compete with the United States in the world market, some of China's leading corporations will risk it all to acquire trade secrets and close the door on new technological advances (Slate, 2009). The severe economic downfall in the 21st century felt around the world is affecting Chinese companies (Slate, 2009). As the situation continues to get

worse, and China's trade networks diminish, China feels the pressure to increase their participation in economic espionage in order to hold a strong hand in the world market and increase its gross domestic products (GDP).

Japan is also among the forerunners of committing economic espionage (Schwartau, 1994). Japan's economic espionage techniques are sponsored by the national trade organization, which sets goals and determines which trade secrets are worthy to steal. They most often carry out these attacks by sending students overseas to gain access to new developing technology. These students are often told for what to look (Slate, 2009; Schwartau, 1994). Most of the techniques used by these students are taking photos and eavesdropping on conversations within university laboratories. In fact, in the 1990s, nearly two entire floors of a Manhattan skyscraper were reportedly occupied by Japanese intelligence spies in order to stay up-to-date on the latest technologies being developed in the United States (Schwartau, 1994). It is also purported that the Japanese spies nearly destroyed the computer technology industry in Silicon Valley (Saxenian, 1994; Schwartau, 1994).

Aviation technology is another form of valuable information that attracts spies (Schwartau, 1994). The most likely country to engage in economic espionage with respect to airplane technology is France. France has had a long standing interest in the airline industry. For example, in order for the French national company of Airbus to gain a competitive advantage, industrial spies often targeted the United States' airline company, Boeing. The French spies used communication receivers to intercept information that was transmitted from test flights conducted by Boeing (Schwartau, 1994). The most common endeavors in which French spies engaged were breaking into hotel rooms, stealing lap tops and brief cases, eavesdropping, and intercepting faxes and emails.

Importance in Researching the Topic

It is important to study economic espionage for a number of reasons. First, the occurrence of economic espionage causes companies great harm, not only financially, but it can also cost a company access to the competitive market. Economic espionage also impacts the GDP of the United States and economic prosperity as a nation. Companies not only invest time and money in the criminal process, but they also lose profits to the possibility of another company producing their product first. Secondly, it is important to study economic espionage because it can help companies safeguard their assets. By understanding the frequency, victimization, and offender characteristics, the information produced can advise at-risk companies and help identify at risk employees.

This study, specifically, is unique in several ways in which it contributes to the literature. Firstly, this study analyzes the period 1996-2011. This study is one of few, if not the only one, that analyses multiple cases of a series of years. Secondly, this study includes all known economic espionage cases during this time period instead of specific cases.

This study also includes content analysis. This study provides offender characteristics in the context of gender and number of offenders involved in each specific criminal act. These characteristics may offer insight into countermeasures and describe the most common demographics of previous offenders. This study also includes victimology. Victimology is the study of victims involved in the crime (Doerner & Lab, 2012). This study analyzed victim-offender relationships and victim demographics such as, company size and SIC code. Lastly, this study includes frequencies of economic espionage in regards to location of occurrences.

Chapter 3: Methods

Overview

This exploratory study examined the nature and extent of economic espionage as reported under 18 USC 1832 criminal prosecutions during the period of 1996-2011. An exploratory study is designed to examine a topic about which little is known, a heavily used method throughout the social sciences. As such, exploratory studies often seek to collect data on a measure that will eventually influence policy. For example, if a researcher wanted to research drug use in order to answer specific questions related to the use and abuse of methamphetamines within the United States, this would be classified as an exploratory study (Maxfield & Babbie, 2010). Exploratory studies also seek to answer questions of the unknown (Maxfield & Babbie, 2010). Because there is little known information pertaining to the nature and extent of economic espionage after the instatement of the Economic Espionage Act, this was an exploratory study. More specifically, this study explored previous Economic Espionage prosecutions to help understand the risk and time investment of foreign espionage.

Research Questions and Hypotheses

There were multiple research questions in mind throughout this study. They included: occurrence rates, offender demographics, victim demographics, and offender relationship status to the victim. These questions were important to address as they will help corporations worldwide become more aware to the problem of economic espionage and the theft of trade secrets. It also will allow for the companies to better safeguard their assets and be better able to combat economic espionage and theft of trade secrets. The following hypotheses exist:

- H_1: High-tech companies are likely to be victimized internally.
- H_2: High-tech companies are likely to be victimized externally.
- H_3: The larger the company, the more likely it is to be victimized by foreign espionage.
- H_4: A company is more likely to be victimized by current employees than a previous employee.

Unit of Analysis

The unit of analysis for this study was criminal court cases prosecuted by the federal courts under 18 USC §1832 between the years 1996 and 2011. The unit of analysis ranged from court dockets, court summaries, newspaper articles, and press releases from the United States Department of Justice. As such, these are social artifacts: "The product of social beings and their behaviors" (Maxfield & Babbie, 2010, p. 96). As a result of the human adversary's criminal behavior, court prosecutions are filed in a public record for review.

Sample Selection/Rationale

This study used entire samples from all cases prosecuted under 18 USC §1832 for the period 1996-2011 (N=105). A population is defined as the entire group a study seeks to examine (Maxfield & Babbie, 2010). Since the variable of interest was Economic Espionage criminal court cases prosecuted by the federal courts under 18 USC §1832 between the years 1996 and 201, and because this study analyzed each court case as opposed to a randomly selected sample, this research method eliminated many sampling issues. Because many sampling issues were avoided, the reliability of the study increased, which in turn strengthened the validity.

Data

The data for this study were criminal cases obtained from PACER (Public Access to Court Electronic Records) in combination with a Google search. Pacer is "an electronic public

access service that allows users to obtain case and docket information from federal appellate, district, and bankruptcy courts" (PACER.gov). Each court maintains its own database within PACER, electronically filing each case. From there, the filings are overseen by the administrative officer of the United States court. This is important in eliminating bias and uploading court dockets which contain important trial information. The search criteria was bounded by the date range of 1996-2011 and, the criminal statutes of §1832. PACER were used to create an exhaustive data set of all cases filed under §1832.

Once the data set was compiled and there was a comprehensive and exhaustive list of cases from 1996-2011 through PACER, other sources were used to find supplemental information. For example, additional information that is not accessible through PACER is company size and SIC code. PACER provided court dockets and information pertaining to sentencing outcomes, offender characteristics and victim characteristics from which the analysis took place. This provided a starting point from which additional searches were conducted to retrieve the remaining information. The Bloomberg Law and WESTLAWNEXT databases were searched via case name and docket numbers. Bloomberg law and WESTLAWNEXT are also legal databases which contain court documents and supplemental information (Bloomberg, 2014; Westlawnext, 2014). From these searches, data was collected on topics such as: offender demographics, victim demographics, victim-offender relationship, sentencing, districts, and date on which the criminal trial was opened. Once the victim demographics were identified, a Google search of the company name was conducted to identify Standard Industrial Classification, company size, offender demographics, and more detailed information regarding the case and offender(s) motive.

Data Collection Plan

The data collection method will be done through archival data analysis. First, a search conducted in PACER with the constraints of 18 U.S.C. §1832 and the date range of 1996-2011 was used to compile a preliminary data set. Second, Bloomberg Law and WESTLAWNEXT were used to validate that the list was exhaustive. Third, Bloomberg Law and WESTLAWNEXT were used to produce court documents. Fourth, consistent with the prior research by Andrijcic and Horowitz (2006), this study examined economic espionage by sector. A content analysis by way of the internet was conducted to provide additional information pertaining to victim characteristics such as standard index code (SIC) and company size based on number of employees. Fifth, offender characteristics were also identified during the content analysis. These characteristics were: number of suspects involved, status of offender(s) employment, gender of the offender, and the offender(s)'sentenced. Sixth, a Google search was used to find supplemental information pertaining to the above variables. Seventh, the Bureau of Labor Statistics was used to classify the size of each company involved. Eighth, this information was entered into an Excel spread sheet and uploaded into SPSS for advanced statistical purposes. All variables are categorical, and coded as either nominal, ordinal, or interval level measures (See Appendix C).

Research Design

The research design for this project is non-experimental. A non-experimental approach is best for this research topic because there is no need for a manipulation or control group (Maxfield & Babbie, 2010). There is no need for a manipulation or control group because the goal of the study, is to describe, not infer the nature and extent of economic espionage. A content analysis was used to produce the information necessary for the data collection process.

Content analysis is defined as the study of recorded data, such as police reports, court filings, and mass media (Maxfield & Babbie, 2010). The content analysis was conducted on the court dockets, court summaries, newspaper articles, and press releases from the United States Department of Justice.

Conceptualization and operationalization will be important to this research project. The conceptual definition of economic espionage used in this study is defined as: theft of any valuable information from a company by an individual, or individuals, for personal or company advancement. The operational definition will be 18 USC 1832. Section 1832, pertaining to Theft of Trade Secrets, is defined as:

> Whoever, with intent to convert a trade secret, that is 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 thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined

under this title or imprisoned not more than 10 years, or both. (B) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000. To verify the reliability of the measures the nature and extent of the problem, offender characteristics, and victim characteristics, interrater techniques will be used to show that the two different researchers can produce the same valid results. Interrater reliability is the use of multiple researchers coding the same data (Maxfield & Babbie, 2010; Johnson & Stevens, 2013). Two different researchers will be provided the identical, relevant information needed for the codification process. If the coding of both researchers is equivalent, the data produced will be accepted as reliable.

Validity issues within this study are minimal, due to the use of official government data and multiple coders. Face validity is strengthened because, taken at the most basic level, these measures "make sense." That is, all cases were prosecuted under 18 USC 1832 as determined by the guidelines established by law and federal prosecutors. Face validity is defined as "the quality of an indicator that makes it seem a reasonable measure of some variable" (Maxfield & Babbie, 2010, p. 139). A good way to measure economic espionage is to use the actual United States' criminal code. Criterion-related validity, which is, "the degree to which a measure relates to some external criterion" was strengthen by comparing the cases identified as dealing with economic espionage to federal court cases that were filed under 18 USC §1832 (Maxfield & Babbie, 2010, p. 140). For example, a list from a non-governmental agency was compared to the list produced by PACER to validate that PACER included all know §1832 prosecutions.

This study also has strong construct validity, the idea of measuring what is intended to be measured (Maxfield & Babbie, 2010). This study is measuring economic espionage. By using United States' criminal code and economic espionage criminal court cases, economic espionage

is actually being measured. Therefore, there is no question in the crime that was committed (based on probable cause) since court cases were filed by the charges brought against the individual or company.

Content validity in this study is difficult to demonstrate. Content validity is "the degree to which a measure covers the range of meanings included within the concept" (Maxfield & Babbie, 2010, p. 141). As stated before, cases go unreported, or are plead down to a different offense. Because this study did not include those cases that went unreported, or plead down to a lesser and different class of offense, content validity is weakened and recognized as an issue.

Human Subject Protections/Ethical Dilemmas

This study does not involve human subjects directly. Because the cases were filed for public review, there were little to no ethical dilemmas or considerations with regards to human subjects and did not require submission to the Institutional Review Board. Although the information is publicly accessible, that does not eliminate any and all ethical concerns. One of the biggest ethical concerns with this study was harm to a company's reputation. To combat this possible ethical concern, the companies' names were not used, and the information gathered and analyzed is anonymous. Likewise, the data did not contain any personal names of victims or defendants. It only report aggregated data.

Chapter 4: Findings

The findings in this study provided insight to the occurrence and different characteristics of 18 U.S.C. 1832 prosecutions from 1996 to 2011. The findings represented frequencies of prosecutions, offender characteristics, and victim demographics. This section is broken down into four sections: extent of the problem, offender demographics, victim demographics, and sentencing outcomes.

Table 1.1 shows the number of 18 U.S.C. 1832 prosecutions during the period 1996 to 2011. As to be expected, the lowest number of prosecutions were delivered at the inauguration of the law in 1996. In 2002, the United States federal court system prosecuted the most cases (N=12). The standard deviation for the number of cases prosecuted for each year is 2.87. Over the 16 year study period, there were a total of 105 prosecuted cases. On average, 7 cases are prosecuted per year.

Table 1.1. Frequency of 18 U.S.C. 1832 Prosecutions by Year (N=105)

Year	Number of Cases	Cumulative	Cumulative %
1996	1	1	.9
1997	4	5	3.8
1998	7	12	6.6
1999	7	19	6.6
2000	5	24	4.7
2001	9	33	8.5
2002	12	45	11.4
2003	5	50	4.7
2004	2	52	1.9
2005	7	59	6.6
2006	7	66	6.6
2007	10	76	9.5
2008	7	83	6.6
2009	6	89	5.7
2010	10	99	9.5
2011	6	105	5.7

Statistical Description	Value
Range	11
Standard Deviation	2.87
High	12
Low	1

Table 1.2 shows the number of 18 U.S.C. 1832 prosecutions in each Federal Circuit Court during the period 1996 to 2011. The 9th Circuit court prosecuted the most cases during this period. Other federal circuit courts with high amounts (greater than six) of prosecutions for the period of 1996 to 2011 are 2nd and 3rd circuit courts. The 4th circuit prosecuted the least amount of cases. There were a total of 105 cases prosecuted in the 11 federal circuit courts during the period 1996 to 2011. On average, each federal circuit court prosecuted 12 cases over the period of analysis. The 2nd and 3rd circuits are located along the eastern coast of the continental United States, while the 9th circuit is located along the western coast of the continental United States. A full map of the federal circuits and case distribution is shown. (Figure 1.3.)

Table 1.2. Frequency of 18 U.S.C. 1832 Prosecutions by Circuit and Year (N=105)

Year	Federal Circuit Court										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1996	0	0	1	0	0	0	0	0	0	0	0
1997	0	0	1	0	1	2	0	0	0	0	0
1998	1	0	2	0	1	0	0	0	1	1	1
1999	0	0	0	0	3	0	2	0	1	0	1
2000	0	1	1	0	0	0	0	0	2	0	1
2001	0	2	1	0	0	2	0	0	3	0	1
2002	2	4	1	0	0	0	0	1	3	1	0
2003	0	0	0	0	0	0	0	0	5	0	0
2004	0	0	0	0	0	0	0	0	2	0	0
2005	0	2	0	0	0	0	1	0	4	0	0
2006	0	1	0	0	0	1	0	1	3	0	1
2007	0	2	3	0	1	0	0	0	4	0	0
2008	1	0	0	0	1	0	1	0	4	0	0
2009	0	0	1	1	0	1	1	0	2	0	0
2010	1	3	1	0	0	2	1	0	1	0	1
2011	0	0	2	0	0	0	2	0	2	0	0
Number of Cases	5	15	14	1	7	8	8	2	37	2	6
% of Total Cases	4.7	14.2	13.3	0.9	6.6	7.6	7.6	1.9	35.2	1.9	5.7

Figure 1.3. Map of United States' Federal Circuits

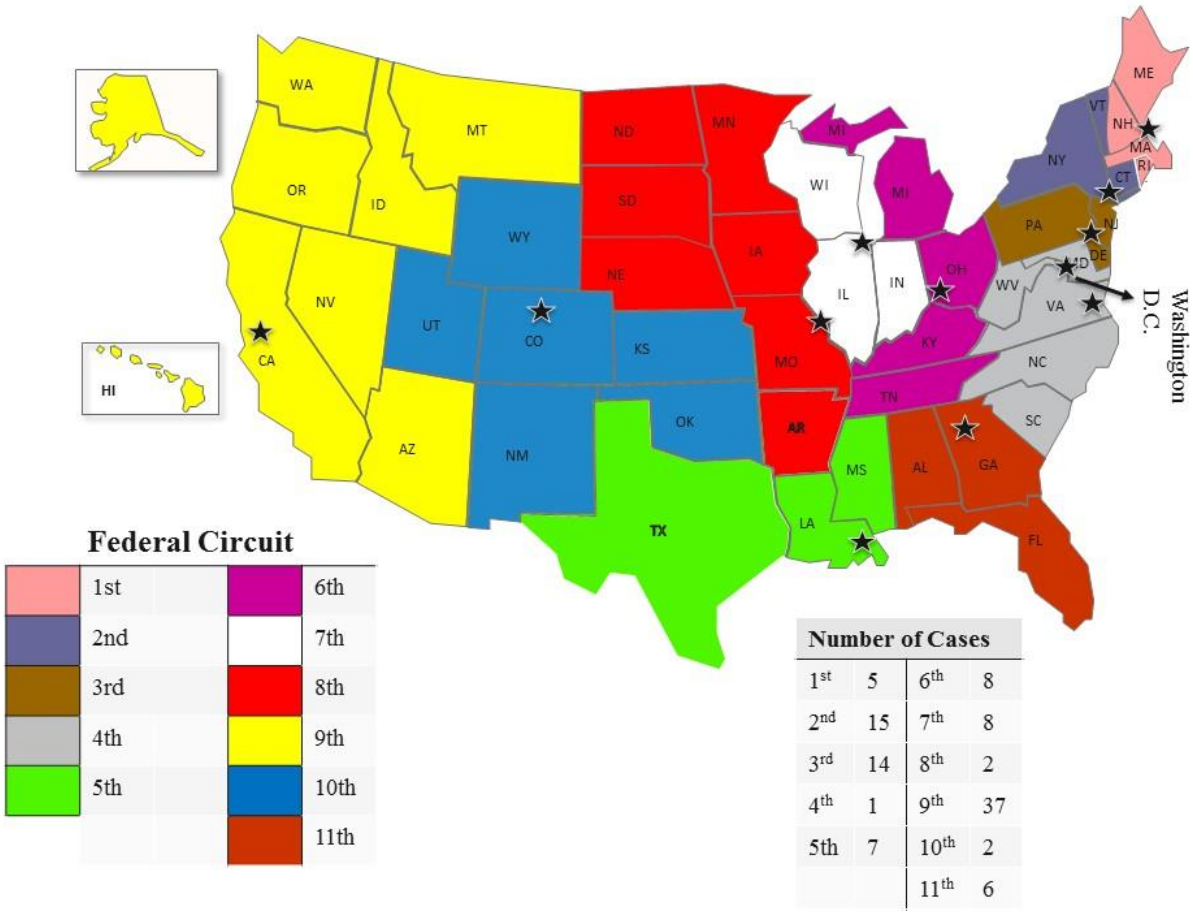

Figure 1.3 provides a visual graphic representation of all US Federal Circuits and the number of §1832 cases prosecuted within each federal circuit. As Figure 1.3 demonstrates, the 2nd, 3rd and 9th district have the highest prevalence of §1832 prosecutions. The 9th district has the highest number of prosecutions with a total number of 37. The other two circuits with high levels of §1832 prosecutions are located along the eastern coast of the continental United States.

Table 2.1 shows the different classifications of companies involved in 18 U.S.C. 1832 prosecutions for the period 1996 to 2011 based on Standard Industrial Classification code. SICs are used by the United States Department of Labor to categorized companies (United States Department of Labor, n.d.). The most common classification involved in 1832 prosecutions were manufacturing companies, represented in 61.1% of the total cases. The second most common classification is services companies, involved 23.3% of the time. Mining and engineering companies are the least likely to be involved in §1832 prosecutions. These companies were involved in 0.9% of the total cases.

Table 2.1. Frequency of 18 U.S.C. 1832 Prosecutions based on Company SIC (N=105)*

Standard Industrial Classification	Number of Cases	Cumulative	Cumulative %
1- Mining and Engineering	1	1	0.9
2- Manufacturing	63	64	61.1
3- Transport, Communications, Electric, Gas, and Sanitary Services	3	67	2.9
4- Wholesale and Retail Trade	2	69	1.9
5- Financial, Insurance and Real Estate	7	76	6.7
6- Services	24	100	23.3
7- Construction	3	103	2.9

*Missing 2

Table 2.2 shows the number of 18 U.S.C. 1832 prosecutions based on company size. During the period 1996 to 2011, the most common company size involved in §1832 prosecutions were those employing 1,000 or more individuals (N=61; 61.0%). The lowest number of §1832 prosecutions involved companies which employed 10 to 19 individuals (N= 2; 2.0%). The average number of §1832 prosecutions for a company within the United States during 1996-2011was 11 prosecutions.

Table 2.2. Frequency of 18 U.S.C. 1832 Prosecutions based on Company Size (N=105)*

Company Size	Number of Cases	Cumulative	Cumulative %
1- (1-4)	8	8	8.0
2- (5-9)	5	13	5.0
3- (10-19)	2	15	2.0
4- (20-49)	4	19	4.0
5- (50-99)	4	23	4.0
6- (100-249)	6	29	6.0
7- (250-499)	6	35	6.0
8- (500-999)	4	39	4.0
9-(1,000+)	61	100	61.0

*Missing 5

Table 3.1 shows the gender of the offenders involved in 18 U.S.C. 1832 prosecutions during the period 1996 to 2011. In 73 cases (69.5%), the offender was male. In 3 cases (2.8%), the offender was female. In 29 cases (27.6%) there were multiple offenders where gender was not easily identifiable due to the lack of information regarding the offender's gender.

Table 3.1. Frequency of Gender in 18 U.S.C. 1832 Prosecutions (N=105)

Gender	Number of Cases	Cumulative	Cumulative %
Male	73	73	69.5
Female	3	76	2.8
Multiple Offenders	29	105	27.6

Table 3.2 shows the offenders' relationship to the offender for 18 U.S.C. 1832 prosecutions during the time period 1996 to 2011. In 41 cases (39.4%), the offender was a current employee of the victimized company. In 42 cases (40.3%), the offender was a former employee of the victimized company. In 18 cases (17.3%), the offender was an external vendor to the victimized company. In 2 of the cases (1.9%), the offender was an acquaintance of a current employee at the victimized company. Lastly, in 1 case (0.9%) the offender was the previous owner of the victimized company.

Table 3.2. Status of Employment to Victimized Company for 18 U.S.C. 1832 Prosecutions (N=105)*

Status of Employment	Number of Cases	Cumulative	Cumulative %
Current Employee	41	41	39.4
Former Employee	42	83	40.3
External Threat-Vendor	18	101	17.3
External Threat Acquaintance	2	103	1.9
Former Owner	1	104	0.9

*Missing 1

Table 3.3 shows the total number of offenders involved in individual prosecutions of 18 U.S.C. 1832 violations during the period 1996 to 2011. The data shows that in most cases (80.9%) there was only one offender involved, followed by two offenders (15.2%). In two cases there were five offenders involved, representing 1.9% of the total cases. There were three offenders involved in one case representing 0.9% of the total cases. Lastly, there was one case which involved ten offenders resulting in 0.9% of the total number of cases.

Table 3.3. Number of Suspects Involved in 18 U.S.C. 1832 Prosecutions (N=105)

Number of Suspects	Number of Cases	Cumulative	Cumulative %
1	85	85	80.9
2	16	101	15.2
3	1	102	0.9
5	2	104	1.9
10	1	105	0.9

Table 4 shows the sentences that the offenders received after being convicted of economic espionage. Table 4 identifies that on average, offenders were sentenced to 20.05 months in prison, 28.81 months of probation, and a $149,477.14 fine during 1996-2011. Prison sentences ranged from 0 to 188 months, probation sentencing ranged from 0 to 60 months, and fines ranged from $0.00 to $7,655,155.00. When sentenced community service, offenders were sentenced, on average, to 3.25 hours of community service. The range was from 0 hours to 150 hours of community service.

Table 4.1. Statistical Analysis of 18 U.S.C. 1832 Prosecution Sentencing (N=105)*

	Prison (Months)	Probation (Months)	Fine (US $)	Community Service (Hours)
Mean	20.05	28.81	149,477.14	3.25
Median	12.00	36.00	3,062.50	0.0
Mode	0	36	100.00	0.0
Std. Deviation	30.487	16.031	856,091.36	20.419
Minimum	0	0	0.00	0.0
Maximum	188	60	7,655,155.00	150

*Missing 21

Chapter 5: Discussion & Conclusions

Economic espionage is a continuing problem for organizations throughout the world (Coskun & Jacobs, 2003). Specifically, within the United States, it is estimated that financial losses exceed $300 billion dollars annually (Almeling et al., 2010). The United States first tried to combat economic espionage by enacting the Uniform Trade Secrets Act of 1979, the National Stolen Property Act of 1948, the World Trade Organization of 1995, and the Trade-Related Aspects of Intellectual Property Rights Agreement of 1994 (Desmet, 1999). These attempts did not yield the desired results; therefore, in 1996, under the Clinton administration, the Economic Espionage Act was signed into law.

The goal of this study was to provide an overview of §1832 prosecutions and its key characteristics of the nature and extent of the problem, offender demographics, victim demographics, and sentencing outcomes during the period 1996 to 2011. The findings from this study describe the nature and extent of the problem, offender demographics, victim demographics, and sentencing outcomes.

Nature and Extent of the Problem

For the period of 1996 to 2011, there were a total of 105 economic espionage cases prosecuted. Table 1.1 represents the number of cases prosecuted each year. At the onset of the law in 1996, there was only one case prosecuted. New legislation creates questions that are not easily answered. This may leave prosecutors hesitant to pursue cases (Desmet, 1999; Effron, 2003). Prosecutors may also not have been able to fully understand the law, or even understand what economic espionage fully entails, therefore, resulting in a low number of cases being prosecuted possibly out of fear of not winning a case. Directly related to numerous questions that are not easily answered by a new law is the burden of proof required in criminal cases.

Proof beyond a reasonable doubt is that there is no other logical explanation based upon the facts presented creating uncertainty (Horowitz, 1997). The burden of proof required in criminal cases coupled with the new legislation may have contributed to the low number of cases prosecuted during the first year of the law (Hill, 2000). Overall, there was a low number of federally prosecuted §1832 cases for the period of 1996-2011.

18 U.S.C. 1832 prosecutions, when compared to all other criminal cases prosecuted in federal courts, account for only a fraction of a percent. For the period of 1996 to 2011, there were a total of 1,044,532 criminal cases filed in the United States' federal district courts ("Case Load Statistics Archive," 2014). As represented by Table 1.1, there were a total of 105 §1832 cases filed and prosecuted. As a result of dividing the §1832 cases by the total cases filled, it is demonstrated that §1832 cases represent .0001% of cases prosecuted for the period of 1996 to 2011.

There are also several other factors that contribute to this underrepresented section of criminal law. First and foremost, economic espionage is an act that is often deceitful and secretive (Simpson, 2013). This results in a number of cases that go unreported or undetected resulting in a high "dark figure of crime." Also, there are crime statistics and information that are unavailable due to missing data. In order for there to be a criminal trial, the crime must be reported to a law enforcement agency. If companies do not know they were victimized, it is impossible for this to be included in official government statistics, leading to the overwhelming issue of missing data. As identified in the literature, most instances of economic espionage are difficult to detect and identify, resulting in a large number of cases that never get reported to a law enforcement agency (Arnulf & Gottschalk, 2013; Myers & Myers, 2003; Simpson, 2013).

From an organizational and business standpoint, there are other significant reasons for underrepresentation of §1832 cases in the federal district court case loads. There are multiple considerations that must be taken into account when a company is making a decision to file criminal charges. A consideration that a company must be aware is the reputational risk involved when filing for criminal charges. Reputational risk is what a company stands to lose when publicly announcing that it has fallen victim to economic espionage (Minott, 2011; Schanz, 2006). When prosecuting economic espionage companies risk losing investors, stock market value, and their reputation. Reputation is the company's trust with stakeholders and other corporations alike in which they do business. For example, if a company lost millions of dollars to one individual's actions, investors and business partners may be hesitant to continue such a cordial relationship. Companies have difficult decisions to make once it has become known that they have fallen victims to economic espionage (Minott, 2011; Schanz, 2006). There need be some form of cost/benefit analysis that takes place in order for the company to understand what is to be lost in order to gain a federal prosecution under the Economic Espionage Act of 1996.

There are also multiple reasons as to why economic espionage is difficult to identify. Firstly, not all acts of economic espionage are intentional; they can be created from natural disasters (Myers & Myers, 2006). For example, a fire or a natural disaster, such as a flood or tornado, can carry valuable information far away from its origin. This may result in someone simply stumbling across a piece of paper with information on it that is extremely valuable. In turn, this loss is nearly impossible to trace, resulting in cases that go unreported to law enforcement agencies. Myers and Myers (2006) also discuss errors and omissions made by employees. These can be something as simple as leaving a computer unlocked after a day's work, or accidently sending an email to the wrong person, or groups of persons. Lastly, the

technological advances made to help prevent and detect instances of economic espionage are not being used to their full potential (Myers & Myers, 2006). Firewalls used by corporations to help safeguard their intellectual property and trade secrets are often so poorly configured that intruders are able to gain access and almost always go undetected. When they go undetected, the intruder is never identified nor is the company ever alerted to the intrusion and the theft of sensitive information. Hence, the issue never is elevated to the level of trade secret theft.

To further explain why the act of economic espionage is underreported, companies often lack the security practices and measures needed to immediately identify the criminal act in order to accurately and efficiently identify the offender (Lippert, Walbym & Steckle, 2013; Walby & Lippert, 2013; Myers & Myers, 2006). For example, most companies lack proper information technology security such as firewalls, anti-virus software, and the lack of password protected programs and files. These infrastructures, or lack thereof, can also include surveillance tools, such as closed circuit television systems and traceable computer use. Lastly, most companies do not have a proper security policy that properly addresses economic espionage (McGee & Byington, 2012).

Another reason that economic espionage is underreported in federal criminal courts is that there are other options available that keep information about the victimization private. For example, the victimized company may file a civil prosecution, or fire the employee suspected of the criminal act (Bucy, Formby, Raspanti & Rooney, 2008). Also, the lack of resources at the federal level may decrease the amount of economic espionage cases that are filled within the federal district court system. Economic espionage cases are often time consuming and take months, if not years, to move through the judicial process. With the lack of financial resources at the federal level, this results in fewer court employees and a more selective manner when

choosing cases to prosecute. For example, when considering financial constraints, prosecutors may be more likely to choose a case where there is a shorter time frame involved from beginning to end, rather than a case that may take years to receive a prosecution (Bucy, Formby, Raspanti & Rooney, 2008; Richman, 2013).

Table 1.2 shows that the western seaboard districts prosecuted the most 18 USC §1832 cases. This may have occurred because the most sought after information by criminals and competing companies pertains to advanced technology (Bergier, 1975; Goldstein, 2007; Schwartau, 1994; Winkler, 1997). The 9th circuit, yielding 37 cases over the 15 year period, is home to Silicon Valley, California (Saxenian, 1994). As identified in the literature, Silicon Valley is home to some of the most technologically sophisticated companies in the world (Saxenian, 1994). Also, Silicon Valley contains high-tech companies that produce goods which are used in mobile devices, televisions, and computer technology. This makes this area a suitable target for economic espionage offenders. The 2nd and 3rd districts also had a high number of prosecutions, a total of 29 cases. The districts are near New York, New York (Mandel, 2013). New York, New York contains a high concentration of large corporations dealing with advanced technologies. This makes this area another suitable target for offenders (Mandel, 2013).

Victim Demographics

There are multiple victim demographics that this study examined, such as standard industrial classification and company size. As demonstrated in table 2.1 and 2.2 this study found that larger manufacturing companies were more likely to be victimized by economic espionage between 1996 and 2011 than other types and sizes of companies identified within this study. Large companies are likely to produce larger profits, and it is known that economic espionage is committed most commonly for financial gains (Myers & Meyers, 2003). Therefore, companies

that produce larger profits are possibly more likely to hold information that yields high monetary value. Furthermore, large companies often have sophisticated and highly specialized security teams that work to protect its assets (Lippert, Walbym & Steckle, 2013; Walby & Lippert, 2013). These larger companies are more likely to detect and identify specifics to the criminal act. With more capital, larger companies are able to invest more time and money into the legal process involved when prosecuting cases. According to Blakeslee (2009), the average costs of criminal court cases dealing with intellectual property law can range from $350,000 to $3,000,000. This demonstrates the lack in monetary sentencing involved in §1832 prosecutions.

Offender Demographics

Criminals who engage in economic espionage have a variety of characteristics. As shown in table 3.1, this study found that most of the offenders in the study were male (69.5%). This finding is highly represented in other criminal justice research. For example, Gottschalk (2012) found that females are represented in only 4% of white collar crime cases. As shown in table 3.1, the majority (79.7%) of the offenders in the study were either a current or former employee of the victimized company. This makes sense as it makes the commission of the criminal act easier by being involved within the company. If an individual has passcodes, badges, or clearance to enter a certain area, it creates a greater likelihood that an individual with this information will be able to access the desired intellectual property (Winkler, 1997; Baker and Benny, 2012). The same is true for former employees. If the companies for which the offender previously worked does not take proper security measures to change passcodes, deactivate badges, or remove clearances from an individual's record, the offender will still have easy access to sensitive information. Also, being either a current or former employee gives the offender knowledge on the exact location that the sensitive information is housed (Baker and

Benny, 2012). Ultimately, being a current or former employee makes it easier to access sensitive information, demonstrating that companies do not have effective policies and procedures to protect against economic espionage.

This study also examined the number of offenders who were involved in each known criminal act of economic espionage. As shown in table 3.2, the offender most often (80.9%) worked alone to gain access and steal the sensitive information. These types of crimes are usually opportunistic in nature where individuals take advantage of an easy opportunity to steal intellectual property (Benson & Simpson, 2009). In these instances most criminals work alone or in pairs to reduce the likelihood of detection (Filstad & Gottschalk, 2012; Holtfreter, 2013). In order for these crimes to be successful, secrecy is the ultimate goal, which is why many companies do not even know they had been victimized (Minott, 2011). If these individuals or groups of individuals are caught, they are prosecuted and sentenced.

Sentencing Outcomes

During the period 1996 to 2011, there were a total of 105 cases brought to federal courts within the United States pertaining to economic espionage, of which 84 resulted in a sentence. Table 4.1 shows the average prison sentence as 20.05 months, an average probation period as 28.81 months, and an average fine as $149,477.14. It should be noted that the average fine may be overestimated due to outliers in the data set. Specifically, there was one criminal case in which there was a fine of $7,655,155 and many cases which yielded no fines. In 34 cases of fraud that the United States' federal courts sentenced the offender with a fine, the average fine was $6,803,438 (U.S. Sentencing Commission, 2013). Although this criminal act is not descriptive or similar to economic espionage, this makes a substantial point: the criminal act of economic espionage is severely under punished in the context of prison sentence and fines. For a

crime where the financial gains are substantial and often exceed millions of dollars, and as compared to other financial crimes within the United States, the fines associated with the criminal act of economic espionage do not represent the severity of the crime. For criminal acts that have the potential for huge profit margins far beyond millions, one would think that the fines and punishments would be much greater. This brings about a substantial point as to why the Foreign and Economic Espionage Penalty Enhancement Act of 2012 was instated; there was a need for increased punishments due the lack of punitive measures being placed on these criminal offenders. This law increased the fines that could be administered to both individuals and organizations (The Foreign and Economic Espionage Penalty Enhancement Act of 2012). It should also be noted that offenders were often sentenced to community service in a total of 77 known cases with an average of 3.25 hours.

Conclusions & Recommendations

This study included archival data analysis on all known §1832 cases for the period 1996 to 2011. This study presents data on the nature and extent of the problem of economic espionage, victim demographics, offender demographics, and sentencing outcomes. Large manufacturing companies are the most likely to be victimized by males acting alone. These offenders are most likely to be current or former employees of the victimized company.

With any type of social science research there are strengths and weakness at the methodological level. Although this technique was exhaustive, there were also some limitations that are important to note. This method allowed for the most time and cost effective way to research this topic. However, this technique did not include any unreported cases; cases that were pled down to a lesser offense under a different federal statute as a result of a pre-trial plea agreement, or cases that were declined for prosecution by the federal government.

This study also relied on the use of official data. This data, however, can fall victim to the "dark figure of crime." The dark figure of crime are all cases that go unreported to law enforcement for a variety of reasons (Biderman & Reiss, 1967). By relying on official government data, this study only provided analysis of known cases. As such, future research could include surveying companies to examine self-reported incite of trade secret theft.

This study failed to include any cases that were not prosecuted under 18 USC § 1832. These cases could have been resolved internally, or the cases went undetected, and the suspects were able to elude prosecution. The literature review showed the depth of the problem and that cases are often pled down to something less than an 18 U.S.C. §1832 prosecution (Edelman, 2011). These cases were not included but are still considered to be part of the problem. Therefore, the depth of the information is limited. Lastly, although interrater reliability is shown, the possibility of coder error still remains.

To counteract these methodological weaknesses, there were many strengths that were unique and provided rich exploratory data. Firstly, this study encompassed all known cases prosecuted under 18 USC §1832. This included 105 cases. These cases are official government data which are limited in bias and are objective in nature (Maxfield & Babbie, 2010). This study used the technique of using the entire population of interest; therefore, there were little validity or reliability threats related to data collection and specifically, sampling. By using the entire population of interest, sampling bias and sampling error was eliminated. However, it could be argued that there was a possibility for coder error; this was eliminated through the demonstration of inter-rater reliability. To increase inter-rater reliability, the results were verified by comparing the codes created by each rater. Lastly, this study analyzed many cases that were prosecuted over a long series of time. This allowed for a comprehensive analysis of the topic issue. This

comprehensive and exhaustive analysis of cases that occurred within a 15 year time span allowed for a full explanation and a true description on the extent of the problem.

There are several suggestions for future research. The literature identifies that the United States are not the only victims to economic espionage. A comparison analysis would provide information as to what countries are doing well and where they need to improve in order to better deter the crime of economic espionage. Secondly, future research should investigate corporations to understand security measures and how they work to protect their information from criminals. This again, would provide insight as to what helps safeguard intellectual property from economic espionage criminals. Also, this would allow companies to see what types of security measures make it easier to detect and identify these types of criminals. Investigating companies would also help remove the "dark figure of crime," to help provide a more detailed description of the nature and extent of the problem.

Regardless of these potential limitations, research on the topic of economic espionage and theft of trade secrets should continue though the future. Future research should look to continually add to this topic by including newer cases as they become available for interpretation. Also, future research should look at the effectiveness of the law, and evaluate whether or not the EEA is doing what it intended to do. Lastly, future research could possibly look at how civil prosecutions compare to criminal prosecutions with respect to deterrence. With future research on these various topics, the crime of economic espionage may wither, leaving companies safe through the EEA.

References

Almeling, D.S., Snyder, D.W., Sapoznikow, M., McCollum, W.E. and Weader, J. (2010). A statistical analysis of trade secret litigation in federal cases. *Gonzaga Law Review, 45,* 291-334.

Alexander, J. M., & Smith, J. M. (2011). Disinformation: A taxonomy. *IEEE, Security and Privacy, 9*(1), 58-63. DOI: 10.1109/MSP.2010.141

Andrijcic, E. and Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk analysis, 26*(4), 907-923. DOI: 10.1111/j.1539-6924.2006.00787.x

Baker, P.R., & Benny, D. J. (2012). *Complete guide to physical security.* Boca Raton, FL: Aurebach Publications.

Barber, R. (2001a). Hacking techniques: The tools that hackers use, and how they are evolving to become more sophisticated. *Computer Fraud & Security, 3,* 9-12.

Barber, R. (2001b). Hackers profiled: Who are they and what are their motivations? *Computer Fraud & Security, 2,* 14-17.

Benson, M. L., & Simpson, S. S. (2009). *White-collar crime: An opportunity perspective.* New York, New York: Routledge.

Bergier, J. (1975). *Secret armies.* New York: The Bob-Merrill Company, Inc.

Biderman, A. D., & Reiss, A. J. (1967). Exploring the "dark figure" of crime. *Annals of the American Academy of Political and Social Science, 374,* 1-15.

Blakeslee, M. (2010). *Pursuing patent infringement litigation at the U.S. international trade commission and in federal district court.* Retrieved from: http://www.sema.org/files/attachments/Government-Affairs-2010-09-Merritt-Blakeslee-ITC-Patent-Infringement-Cases.pdf

Bloomberg. (2014). Bloomberg law. Retrieved June 22, 2014, from: http://about.bloomberglaw.com/

Butler, R. P. (2005). Intellectual property defined. *Knowledge Quest, 34*(1). 41-42.

Carte, N. E. (1988). Patent applications: Need and timing can be as critical as validity. *High Technology Business, 8*(12), 14-15.

Coskun, S.A and Laurence, J. (2003). Counteracting global industrial espionage: A damage control strategy. *Business and society review, 108*(1), 95-113.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons, 48,* 233-240.

Crawford, J., & Strasser, R. (2008). Management of infringement risk of intellectual property assets. *Intellectual Property & Technology Law Journal, 20*(12), 7-10.

Davids, K. (1995). Openness or secrecy? Industrial espionage in the Dutch Republic. *The journal of European economic history, 24*(2), 33-348.

Desmet, T.O. (1999). The economic espionage act of 1996: Are we finally taking corporate spies seriously? *Houston journal of international law, 22*(1), 94-126.

Doerner, W. G., & Lab, S. P. (2012). *Victimology* (6th ed.). Burlington, MA: Anderson Publishing.

Dole, R. F. (2010). The uniform trade secrets act: Trends and prospects. *Hamline Law Review, 33*(3), 409-442.

Dol.gov. (N.D.). Department of Labor. Retrieved from: https://www.osha.gov/pls/imis/sic_manual.html

Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified as amended at 18 U.S.C. §§ 1831-1839 (2000)).

Edelman, W.J. (2011). The "benefit" of spying: Defining the boundaries of economic espionage under the economic espionage act of 1996. *Stanford law review, 63*(2), 447-474.

Effron, R.J. (2003). Secrets and spies: Extraterritorial application of the economic espionage act and the TRIPS agreement. *New York university law review, 78*, 1475-1517.

Fialka, J.J. (1997). While America sleeps. *The Wilson quarterly, 21*(1), 48-63.

Foreign and Economic Espionage Penalty Enhancement Act, Pub. L. No. 112-269, 126 Stat. 2442 (2013).

Fraumann, E. (1997). Economic espionage: Security missions redefined. *Public administration review, 57*(4), 303-308.

Garcia, M. L. (2005). *Vulnerability assessment of physical protection systems*. Burlington, Massachusetts: Elsevier Butterworth-Heinemann.

Goldstein, P. (2007). *Intellectual Property: Tough new realities that could make or break your business*. London, England: Penguin Group

Gottschalk, P. (2012). Gender and white-collar crime only four percent female criminals. *Journal of Money Laundering Control, 15*(3), 362-373. doi: 10.1108/13685201211238089

Hannah, D.R. (2005). Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. *Organization science, 16*(1), 71-84. DOI: 10.1287/orsc.1040.0113.

Hamilton, P. (1967). *Espionage and Subversion on an Industrial Society.* London, England: Hutchinson & Co. Ltd.

Hemphill, T. (2004). The strategic management of trade secrets in technology-based firms. *Technology analysis and strategic management, 16*(4), 479-494. DOI: 10.1080/0953732042000295793.

Hill, S. (2000). To prosecute or not. *The World Today, 56*(8/9), 35-37.

Johnson, B. R., & Stevens, R. S. (2013). The regulation and control of bail recovery agents: An exploratory study. *Criminal Justice Review, 38*(2), 190-206. DOI: 10.1177/0734016812473823.

Kingston, W. (2006). Trademark registration is not at right. *Journal of Macromarketing, 26*(17), 17-26. DOI: 10.1177/0276146705285683.

Lippert, R. K., Walby, K., & Steckle, R. (2013). Multiplicities of corporate security: Identifying emerging types, trends and issues. *Security Journal, 26*(3), 206-221. doi: 10.1057/sj.2013.12

Machlis, S. (1997). Levi Strauss caught with its pants down. *Computerworld, 31*(18), 1.

Mandel, M. (2013). Building a digital city: The growth and impact of New York City's tech/information sector. *Bloomberg Technology Summit.* Retrieved from: http://www.mikebloomberg.com/files/buildingadigitalcity.pdf

Maxfield, M., & Babbie, E. (2010). *Research methods for criminal justice and criminology (6th e.d.).* Belmont, CA: Wadsworth.

Maxwell, R. (1998). What is a spy to do? *Social text, 56*, 125-141.

Minott, N. (2011). The economic espionage act: Is the law all bark and no bite? *Information and communications technology law, 20*(3), 201-224. DOI: 10.1080/13600834.2011.603963.

O'Hara, G. (2010). Cyber-Espionage: A growing threat to the American economy. *The catholic university of America CommLaw conspectus, 19,* 1-44.

PACER. (N.D.). *Public Access to Court Electronic Records.* Retrieved February 2, 2014, from: http://www.pacer.gov/

Pacini, C.J., Placid, R., Wright-Isak, C. (2008). Fighting economic espionage with state trade secret laws. *International journal of law and management, 50*(3), 121-135. DOI: 10.1108/17542430810877454.

Pellissier, R., & Nenzhelele, T. E. (2013). Towards a universal competitive intelligence process model. *SA Journal of Information Management, 15*(2), 567-573. DOI: 10.4102/sajim.v15i2.567.

Power, R., and Forte, D. (2006). Thwart the insider threat: A proactive approach to personnel security. *Computer fraud and security, 7,* 10-15. DOI: 10.1016/S1361-3723(06)70400-6.

Pushkar, R.S. (2005). Corporate trade secrets: Protecting company assets. *Contract management, 45*(7), 24-27.

Quinto, D. W., & Singer, S. H. (2012). *Trade secrets: Law and practice.* New York, NY: Oxford University Press, Inc.

Ronde, T. (2011). Trade secrets and information sharing. *Journal of economics and management strategy, 10*(3), 391-417.

Saxenian, A. (1994). Lessons from Silicon Valley. *Technology Review, 97*(5), 42-51.

Schanz, K. (2006). Reputation and reputational risk management. *The Geneva Papers, 31,* 377-381. doi: 10.1057/palgrave.gpp.2510092.

Schwartau, W. (1994). *Information warfare.* New York, NY: Thunder's Mouth Press.

Schweizer, P. (1993). *Friendly spies: How America's allies are using economic espionage to steal our secrets.* New York, NY: Atlantic Monthly Press.

Sepura, K. (1998). Economic espionage: The front line of a new world economic war. *Syracuse journal of international law and commerce, 26,* 127-152.

Silbert, S. (2008). Defining trademarks. *Los Angeles Lawyer, 31*(5), 14.

Slate, R. (2009). Competing with intelligence: New direction in China's quest for intangible property and implications for homeland security. *Homeland Security affairs, 5*(1), 1-27.

United States Department of Justice. (2014). *U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage.* Retrieved from: http://www.justice.gov/opa/pr/2014/May/14-ag-528.html

UScourts.gov. (N.D.). *Federal Caseload Statistics.* Retrieved from: http://www.uscourts.gov/Statistics/FederalJudicialCaseloadStatistics.aspx

Vashisth, A., & Kumar, A. (2013). Corporate espionage: The insider threat. *Business Information Review, 30*(2), 83-90. DOI: 10.1177/0266382113491816.

Walby, K., & Lippert, R. (2013). Introduction to special issue on new developments in corporate security and contract private security. *Security Journal, 26*(3), 201-205. doi: 10.1057/sj.2013.11

Westlawnext. (2014). Westlawnext. Retrieved from: https://1.next.westlaw.com/Session/SignOn.html?bhcp=1

Winkler, I. (1997). *Corporate espionage: What it is, why it's happening in your company, what you must do about it.* Rocklin, CA: Prima Publishing.

Appendix A:

SECTION 1. SHORT TITLE.

This Act may be cited as the `Economic Espionage Act of 1996'.

TITLE I--PROTECTION OF TRADE SECRETS

SEC. 101. PROTECTION OF TRADE SECRETS.

(a) IN GENERAL- Title 18, United States Code, is amended by inserting after chapter 89 the following:

CHAPTER 90--PROTECTION OF TRADE SECRETS

`Sec. 1831. Economic espionage

`(a) IN GENERAL- Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--

`(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

`(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

`(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

`(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

`(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as

provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

`(b) ORGANIZATIONS- Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

`Sec. 1832. Theft of trade secrets

`(a) Whoever, with intent to convert a trade secret, that is 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 thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

`(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

`(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

`(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

`(4) attempts to commit any offense described in paragraphs (1) through (3); or

`(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

`(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

`Sec. 1833. Exceptions to prohibitions

`This chapter does not prohibit--

`(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

`(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

`Sec. 1834. Criminal forfeiture

`(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States--

`(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

`(2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

`(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this section.

`Sec. 1835. Orders to preserve confidentiality

`In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

`Sec. 1836. Civil proceedings to enjoin violations

`(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

`(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

`Sec. 1837. Applicability to conduct outside the United States

This chapter also applies to conduct occurring outside the United States if--

`(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

`(2) an act in furtherance of the offense was committed in the United States.

`Sec. 1838. Construction with other laws

`This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

`Sec. 1839. Definitions

`As used in this chapter--

`(1) the term `foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

`(2) the term `foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

`(3) the term `trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--

`(A) the owner thereof has taken reasonable measures to keep such information secret; and

`(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

`(4) the term `owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.'.

(b) CLERICAL AMENDMENT- The table of chapters at the beginning part I of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following:

1831'.

(c) REPORTS- Not later than 2 years and 4 years after the date of the enactment of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601).

Passed by Congress: October 2, 1996

Signed into law by President Clinton: October 11, 1996

Appendix B:

One Hundred Twelfth Congress
of the
United States of America
AT THE SECOND SESSION

Begun and held at the City of Washington on Tuesday,

the third day of January, two thousand and twelve

An Act

To amend title 18, United States Code, to provide for increased penalties for foreign and economic espionage, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the `Foreign and Economic Espionage Penalty Enhancement Act of 2012'.

SEC. 2. PROTECTING U.S. BUSINESSES FROM FOREIGN ESPIONAGE.

(a) For Offenses Committed by Individuals- Section 1831(a) of title 18, United States Code, is amended, in the matter after paragraph (5), by striking `not more than $500,000' and inserting `not more than $5,000,000'.

(b) For Offenses Committed by Organizations- Section 1831(b) of such title is amended by striking `not more than $10,000,000' and inserting `not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided'.

SEC. 3. REVIEW BY THE UNITED STATES SENTENCING COMMISSION.

(a) In General- Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of offenses relating to the transmission or attempted transmission of a stolen trade secret outside of the United States or economic espionage, in order to reflect the intent of Congress that penalties for such offenses under the Federal sentencing guidelines and policy statements appropriately, reflect the seriousness of these offenses, account for the potential and actual harm caused by these offenses, and provide adequate deterrence against such offenses.

(b) Requirements- In carrying out this section, the United States Sentencing Commission shall--

(1) consider the extent to which the Federal sentencing guidelines and policy statements appropriately account for the simple misappropriation of a trade secret,

including the sufficiency of the existing enhancement for these offenses to address the seriousness of this conduct;

(2) consider whether additional enhancements in the Federal sentencing guidelines and policy statements are appropriate to account for--

(A) the transmission or attempted transmission of a stolen trade secret outside of the United States; and

(B) the transmission or attempted transmission of a stolen trade secret outside of the United States that is committed or attempted to be committed for the benefit of a foreign government, foreign instrumentality, or foreign agent;

(3) ensure the Federal sentencing guidelines and policy statements reflect the seriousness of these offenses and the need to deter such conduct;

(4) ensure reasonable consistency with other relevant directives, Federal sentencing guidelines and policy statements, and related Federal statutes;

(5) make any necessary conforming changes to the Federal sentencing guidelines and policy statements; and

(6) ensure that the Federal sentencing guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

(c) Consultation- In carrying out the review required under this section, the Commission shall consult with individuals or groups representing law enforcement, owners of trade secrets, victims of economic espionage offenses, the United States Department of Justice, the United States Department of Homeland Security, the United States Department of State and the Office of the United States Trade Representative.

(d) Review- Not later than 180 days after the date of enactment of this Act, the Commission shall complete its consideration and review under this section.

Speaker of the House of Representatives.

Vice President of the United States and

President of the Senate.

Appendix C:

CODEBOOK

The size of the victimized company was broken down into a series of numerical ranges:

- 1-4 employees (1)
- 5-9 employees (2)
- 10-19 employees (3)
- 20-49 employees (4)
- 50-99 employees (5)
- 100-249 employees (6)
- 250-499 employees (7)
- 500-999 employees (8)
- 1,000 or more employees (9)

This system of classification was taken directly from the United States' Bureau of Labor Statistics, specifically, the Bureau of Labor Statistics national business employment dynamics data by firm size class. This is used because it is the most commonly accepted measurement of business size within the United States.

The status of the offenders' employment was coded and categorized as follows:

- Current employee/internal threat (1)
- Ex-employee/external threat (2)
- External vendor (3)
- External threat who is an acquaintance of current employee (4)

These classifications were chosen so that each case would fall into one of these four categories.

Gender of the offender was coded as follows:

- Male (1)
- Female (2)
- Multiple offenders (3)

Standard Industrial Classification was coded as follows:

- Mining and engineering (1)
- Manufacturing (2)
- Transport, communications, electric, gas, and sanitary services (3)
- Wholesale and retail trade (4)
- Financial, insurance, and real estate (5)
- Services (6)
- Construction (7)

The number of suspects involved in each §1832 prosecution was coded as follows:

- The total number of suspects were totaled and recorded in numerical form.
    - 1 offender (1)
    - 2 offenders (2)
    - 3 offenders (3)
    - 4 offenders (4)
    - 5 offenders (5)
    - 6 offenders (6)
    - 7 offenders (7)
    - 8 offenders (8)

- 9 offenders (9)
- 10 offenders (10)

Federal Circuit was coded as follows:

- First Circuit (1)
- Second Circuit (2)
- Third Circuit (3)
- Fourth Circuit (4)
- Fifth Circuit (5)
- Sixth Circuit (6)
- Seventh Circuit (7)
- Eighth Circuit (8)
- Ninth Circuit (9)
- Tenth Circuit (10)
- Eleventh Circuit (11)

The year in which each individual prosecution took place was coded in its numerical form. For example, 1996 was code as 1996.

Prison and probation sentences were coded numerically by the number of months each offender received during sentencing.

Community service was coded numerically by the number of hours each offender received during sentencing.

Lastly, the fine that each offender received at sentencing was coded numerically and in United States' dollars.