**Economic Espionage**

**Introduction**

Economic espionage is a threat that has been in the commerce sector for a while until October 1996, where the US recognized it and responded by signing the Economic Espionage Act into law. The following essay will exploit economic espionage, its characteristics, how it affects, how, examples, and the measures taken to stop this criminal offence.

**What is Economic Espionage?**

Economic espionage is defined as the unlawful targeting and theft of sensitive information from an organization, business or company, such as intellectual property and trade secrets. This could also involve the outright theft of invaluable information in several areas, including government policies, technology and finance. This concept can also be state-sponsored and entail motives other than profits or other financial gains (Danielson, 2008).

Economic and industrial espionage takes place in two main concepts. The purpose of espionage is to gather vital information about one or more organizations. As mentioned above, this information is often intellectual property like information of industrial manufacture, recipes and formulas, techniques and ideas (Danielson, 2008). It could also be operational information such as policies, prospective bids, planning or marketing strategies, changing positions, customer datasets, marketing, sales, research and development, pricing, and production location. It can also involve activities such as blackmail, technological surveillance, bribery and trade secrets. Commercial organizations can also be targets; for example, they could use them to find information on a tender for a government contract (Danielson, 2008).

The Federal Bureau of Investigation defines economic espionage differently. They explain it as the act of collective intelligence or foreign power-sponsored that is directed at the U.S government, persons, establishments and corporations designed to illegally influence vital economic policy decisions or unlawfully obtain sensitive economic, financial or trade information, critical technologies, and proprietary economic information (Tucker, 1997). These thefts can provide foreign entities with important proprietary economic information at a cost for the development and research causing significant losses in their economy (Danielson, 2008).

There are three main ways that the FBI has divided how foreign competitors conduct economic espionage. These include; recruiting people working in the areas they want to rob like U.S companies, research institutions who often share the same national background, using methods like cyber attacks, wiretapping and bribery, and establishing fake innocent relationships with U.S companies to help gather economic intelligence which include trade secrets which they use for their own gain. The FBI advises such organizations to have proactive plans to ensure security for their trade secrets, secure electronic and physical versions of intellectual property, and train the employees appropriately (Tucker, 1997) (Danielson, 2008).

**Who is affected by Economic Espionage?**

Despite advances made by major companies in cybersecurity to ensure that they don’t get robbed of their intellectual information, they are still of great interest to foreign threat factors. Major companies tend to deal with energy, environmental protection, high-end manufacturing, information and communication technology, biotechnology and, most importantly, defence (Carr & Gorman, 2001). They are often affected in the terms where the software supply chain might be infiltrated. This threatens the U.S critical infrastructure and can also affect other sectors that work together with the companies (Carr, & Furniss, 1999). Businesses are mostly affected to obtain their planning and strategy information by other rival companies. For customers, they are mainly affected when the companies they depend on getting hacked, and their customer service is obtained. This information includes their names, credit card information and, in some cases, their home addresses or current locations (Carr & Gorman, 2001).

**How are they affected?**

There are numerous cases often involving the hacking of the software supply chain, therefore disrupting the organization's finance. Affecting major companies, which in such cases are parent companies, affects other companies working under their financial support. Their information and other important information can be accessed and making the whole chain of companies affected by the theft (Carr & Gorman, 2001). Their customers and other partnering companies might ask for a legal fee because of their information's exposure through their incompetence or lack of enough cybersecurity to protect their clients and partners' information. This generally ruins the company's reputation, and it can even interrupt ongoing businesses and upcoming dealings (Carr, & Furniss, 1999).

When businesses lose the information that makes them better than others, it is hard for them to strategize all over again to ensure that they stay on top of the game (Carr, & Furniss, 1999). The fact that many rival businesses will be willing to pay a good amount of money t access that information makes it even harder for them because competition will come from one or two companies but from all possible businesses venturing in the same business as them. This causes business disruption and losses to the companies and businesses (Carr & Gorman, 2001).

Most customers buying products rarely have time to pick up their products from where they buy them from. This has become more common, especially with the ongoing pandemic whereby most countries are in lockdown and are advised to social distance. Therefore for the bought products to reach the customers, they have to be delivered at their doorsteps (Carr & Gorman, 2001). This means that when customers order their products, they give personal information like their credit card information to pay remotely, their full names and their home address. This procedure does not make any of the people feel safe if the company or business is cyber-attacked. Security for every citizen and customer is important, but economic espionage makes maintaining their security hard because of access to personal information (Carr & Gorman, 2001) (Carr, & Furniss, 1999).

**Signs of Economic Espionage.**

There are several warning signs that employees or clients are spying or stealing delicate information from a business. The first one is when employees work odd hours without authorization from the management or those in charge. This often means that they have activities that they don’t want other employees to know about to a business getting possible threats of economic espionage. They often take proprietary or other sensitive information home in hardcopy or drives without need or authorization. Unnecessary copying of classified information is also a red light for any company at risk (Danielson, 2008).

Most of these personalities tend to disrespect protocol, access restricted websites, surf unauthorized searches, and download confidential information from the company’s database. The employees often take unexplained trips to unknown destinations or foreign countries. Employees who engage in suspicious personal contacts with unauthorized individuals like competitors or business partners can also be suspects in this case. Such people can also afford to buy things that their sources of income can’t afford. In most cases, they will be noticed to be extremely concerned about being investigated and leaving listening devices and cameras around to obtain all the information they can get their hands on(Danielson, 2008).

**Examples from U.S. cases**

1. **The espionage case involving Canada in 2013**

In 2013, Edward Snowden, the American whistleblower, retrieved documents that revealed that Canada had set up spies around the world and, in that way, conducted espionage against trading partners at the request of the U.S Security Agency. The documents from NSA being reported revealed that Canada was involved with the major American Intelligence. It was concluded that the attack would have been possible because of both CSEC and NSA for the lack of proper oversight (Mayers, 2018) (Van, 2001).

1. **Operation Night Dragon**

In 2011, Chinese hackers broke into the computer systems of five multinational oil and gas companies. The other seven companies fell victim secondarily from the attack on the five even though the effects were not clear. None of the companies confirmed which companies were affected by the espionage (Van, 2001).

1. **Kodak**

Back in the 1990s, Kodak fell victim f industrial espionage whereby one employee from the company Harold Worden, 56 years old, stole Kodak’s property that was worth millions of dollars. He had worked in the company for more than 30 years and had not returned confidentiality documentation when he left the company. He tried to sell the information and property that he had stolen from Kodak to other rival companies while trying to start his own consulting firm. He was sentenced to 15 months in prison and fines that amounted to over fifty thousand dollars in 1997 (Van, 2001).

1. **IBM**

In the 1990s, IBM won a case against Hitachi and two of its employees for industrial espionage. Hitachi had conspired with the two employees to steal confidential data from IBM and take it to Japan. Hitachi and its partners who had conspired together pled guilty to the charges. The two employees were charged ten thousand dollars and four thousand dollars while the company was also charged ten thousand dollars fine for their espionage participation (Van, 2001).

1. **Avery Dennison**

Between 1989 and 1997, a business from Taiwan steals trade secrets from a company in Ohio called Avery Dennison. This company was one of the nation’s best producers of adhesive products that are used in things like diaper tape and postage stamps. In 1999, the defendants were taken to court and plead guilty and pay forty million dollars for damage control to the company. This was the first case in trial after the Espionage Act was minted in 1996 (Van, 2001).

**Economic Espionage is not only limited to within the United States.**

In 2013, leaked documents showed that Canada's electronic intelligence was targeting the Brazilian government that threatened to ruin the relationships between the two countries. These leaked documents were the secretive Communications Security Establishment Canada (CSEC) into the public spotlight. The documents were part of a collaboration with Globo. The impact of these revelations would be bad for both Canada and Brazil and would ruin their economic relationships. However, the leak is solved and saves the two countries a lot of trade wars and inconveniences (Van, 2001).

**How is Economic Espionage punishable by law in the United States?**

The punishment for espionage depends on the offence and the amount of damage that could be caused by the theft. Economic espionage can be very serious in most cases, and therefore the punishments are as serious as the offences are (Fischer, 2001). Industrial espionage can be very costly. The penalties for stealing trade secrets can be as high as one hundred thousand dollars, especially those affecting more than one country and a sentence of up to 15 years imprisonment.

If the stolen documents are for personal gains, the convicted can face a ten-year sentence or be fined. For companies, the punishment is more severe because the effects are more severe. The company can be fined as much as ten million dollars for stealing trade secrets for other states. In cases of smaller fines, the companies are often charged up to five million dollars if it was for the own company’s own benefits (Fischer, 2001).

**Conclusion**

Economic espionage is a bad habit that is still growing despite the government and companies' measures to stop it or at least reduce it. For this problem to be solved, people should learn to work hard for their pay and profits instead of gaining from the loss of losing others, and that lesson should be instilled in people at a young age.

**References**

Danielson, M. E. (2008). Economic espionage: A framework for a workable solution. *Minn. JL Sci. & Tech.*, *10*, 503.

Carr, C., & Gorman, L. (2001). The revictimization of companies by the stock market who report trade secret theft under the Economic Espionage Act. *The Business Lawyer*, 25-53.

Carr, C., Morton, J., & Furniss, J. (1999). The economic espionage act: Bear trap or mousetrap. *Tex. Intell. Prop. LJ*, *8*, 159.

Fischer, J. M. (2001). An Analysis of the Economic Espionage Act of 1996. *Seton Hall Legis. J.*, *25*, 239.

Mayers, A. M. (2018). *A study on how cyber economic espionage affects US national security and competitiveness* (Doctoral dissertation, Northcentral University).

Tucker, D. S. (1997). The Federal Government's War on Economic Espionage. *U. Pa. J. Int'l Econ. L.*, *18*, 1109.

Van Arnam, R. C. (2001). Business war: Economic espionage in the United States and the European Union and the need for greater trade secret protection. *NCJ Int'l L. & Com. Reg.*, *27*, 95.