International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 06 | June 2023 www.irjet.net p-ISSN: 2395-0072

Computer Forensics And Investigating Corporate Espionage

Prof. Mahesh Rajaram Kudalkar

Assistant Professor, D.G. Ruparel College of Arts, Science and Commerce, Mumbai, India

---

Abstract - *Research studies the usefulness of computer forensics while investigating corporate espionage, With the help of past cases this research explains the need of Economic Espionage Act of 1996 and recommends the critical safety measures to be implemented in any organization to prevent the theft of trade secrets or intellectual property.*

***Key Words*: Computer Forensics, Espionage, Economic Espionage Act 1996, Digital Information, Theft, Commercial Secrets**

1.INTRODUCTION

Every company in each business is vulnerable to the rising threat of corporate espionage and theft of proprietary secret. We work to protect our client's intellectual property. Corporate espionage is on the rise globally, and businesses and nations are employing whatever moral or immoral tactics necessary to gain the information that will give them a competitive edge or financial advantage over the different competitive organizations and business.

Corporate espionage is the stealthy and illegal method of investigating competitors businesses and to gain a business advantage. A trade secret, such as a private product specification, a secret recipe, or a roadmap of corporate goals, could be the subject of a criminal investigation. Industrial spies frequently just gather any information that their company can use to its benefit.

An industrial spy could pose a threat from within the corporate organisation, for example if they were hired by the corporation with the express purpose of spying or a unhappy employee who sells information for personal gain or revenge. Social engineering techniques, such as persuading an employee into disclosing their passwords or credentials, are another way that spies may intrude.

Spies sometimes needs to physically breach the target organization's security and investigate the premises, when it is very hard to compromise a employee or obtain a information. In such cases, a spy might search for critical information in waste baskets or copy files from hard drives of unattended computers. now a days, the intrusion happens through the corporate network. The company's network is typically targeted via an attack that involves breaching the firewall to get initial network access, followed by the deployment of an advanced persistent threat (APT) or Remote Access Trojan (RAT) to continue data theft. If a hacker gains access to an employee's cell phone by leaving the phone in a boardroom, the ability of cell phones to record and broadcast can also be exploited, for example, monitoring a meeting remotely. Now a days different recording devices are also available in a variety of items including eyeglasses, pens and USB sticks.

2 ORIGINS

The history of economic and industrial espionage is extensive. Some consider Father Francois Xavier from China, who revealed porcelain production techniques to Europe in 1712, to be the first and earliest instance of industrial espionage.

Historically many cases have happened of industrial espionage between Britain and France. Credit to Britain's emergence as an "industrial creditor", the second decade of the 18th century recorded the emergence of a large-scale state sponsored effort to take British industrial technology to France. Witnesses confirmed both the persuade the trades persons abroad and the placing of apprentices in England. Protests by ironworkers and steelworkers against the export of skilled industrial workers.

English legislation aimed at preventing this method of economic and industrial espionage, although this did not prevent Samuel Slater from bringing British textile technology to the United States in 1789, to catch up with the new technology of the Britain, the government of US in the eightieth and nineteen centuries actively encouraged intellectual piracy.

3. TYPES OF INDUSTRIAL ESPIONAGE

The term "industrial espionage" refers to a variety of methods, including:

- visiting a competitor's property without authorization in order to access their files.
- Posing as a worker for a rival company to get corporate trade secrets and other confidential information.
- Listening in on a rival.
- Breaking into a rival's computers.
- Launching a malware attack on a rival's website.

But not every corporate espionage is dramatic. Much can be as simple as an employee transferring trade secrets from

one company to another a disgruntled employee, or an employee who has been fired by a company and takes information with them such as customers records, company data or secret etc, which they shouldn't.

Then there is competitor's intelligence which is, also called as in information security terms, the white-hat hacking of corporate businesses. Competitive intelligence companies say they're legal and have authority, to gather and analyse information which is largely public that can affect their clients' security mergers and acquisitions, or new government regulations, blogs and social media. They might research the background of a executive and they will say not digging up any dirt, but to try to understand their motives and to predict their behaviour in given situation. That's everything in the theory, though sometimes, the line separating these methods from criminal intend can be very thin.

It's also true that not all corporate espionage involves turning employees or assigning spies on other businesses. Often governments get into the game too, especially different countries where many businesses are state-owned and managed solely by the state the administration views necessary economic development as an important national goal. As a result, other governments drawn to such economic development from various degrees, one of the main motivations President Trump has given for escalating a trade war with China has been to fight against the theft of American trade secrets. When states are involved in the process of espionage, the term used here is economic espionage.

3.1 Why Companies Don't Prosecute?

Corporate espionage may involve inside information and is very hard to prove in the court of law. Because of this, many companies don't prosecute.

Reasons for this include:

- Differing laws in each country and foreign governments making it difficult to hold anyone responsible

- Fear of reputation damage or damage to the company's financial status if it becomes public knowledge that they were victimized

All the customers knows that a company is responsible for the security of its their data, so a leak or a theft of that data can cause legal issues and fines, and severe reputation and PR issues.

3.2 Case Where Kodak Trade Secrets Were Stolen!!!

Harold Worden was a employee of the Kodak Corporation retired from his duty after a 30 years of his employment. He managed the project for the new product known as the 401 machine for the final five years of his employment at Kodak. This was the new machine explicitly design to produce the clear plastic base in low cost which was used in consumer film. The base was lined with blend using a proprietary formula that improves the quality of the photographs. When Worden retired, not only he took hundreds of documents marked as "confidential" about the 401 machines development, but also he recruited his replacement to continue providing proprietary information from Kodak Corporation.

A Kodak representative said the numerous plans, drawings and important documents which was taken by Worden were worth millions of dollars to the company, even though Worden stated that by the time of his arrest had only received around $25,000 for selling that information. The risk to the market share because of Harold Worden's scheme could have been in the billions of dollars.

In August 1997, Harold entered a plea of guilty to one felony count of transporting stolen goods. He was sentenced to one-year imprisonment, three months of home confinement, three years of probation, and a fine of $30,000 in November 1997. Kodak has a lawsuit pending against him for financial recovery.

A week after Harold was given his punishment, Kodak accused a different retired worker of giving trade secrets to what was then 3M's photographic film subsidiary in Ferraina, Italy.

4. UNITED STATES OF AMERICA [ECONOMIC ESPIONAGE ACT OF 1996]

Economic Espionage Act of 1996 is the U.S. federal law which control corporate espionage. The law made stealing proprietary secrets (as opposed to classified or national defense information) a federal crime for the first time in history, and structures a detailed definition of what comprise a trade secret. Additionally, it lists the harsh punishments for corporate espionage, including fines of millions of dollars and lengthy prison terms. Most of the heaviest legal penalties are meted out to anyone who divulge trade secrets to foreign businesses or governments, and indeed the very first trial sentence under the law involved a Boeing plane engineer who had sold trade secrets to China.

It is significant to highlight that not all instances of corporate espionage result in criminal charges. The US Department of Justice has issued guidelines on which cases to pursue, and they are as follows:

- The scope of the criminal intend, including evidence of involvement by a foreign establishment, or a foreign actor.

- The extent of the organization's secret owner's economic depreciation

• What kind of trade secret was stolen

• The efficiency of the civil remedies that are accessible

• The potential value of the prosecution

But keep in mind just because an action doesn't merit for prosecution doesn't make it legal, and violations can be served as the basis for lawsuits in civil court. Additionally, several states have corporate espionage statutes that are stricter than federal law; for example, the famous "pretexting" case involving Hewlett-Packard involved illegal exploits. under U.S. federal law but was in California's state law, and resulted in about $14 million fine.

5. USE OF COMPUTER FORENSICS IN INVESTIGATIONS

In civil cases or corporate investigations digital forensics is used for the electronic discovery or eDiscovery. Forensic investigation methods are also similar to the one's which are used in criminal investigations, mostly with different legal requisite and barrier. Outside the court of law, with the help of digital forensics evidence can be found in corporate investigations.

The goal of digital forensics is to track down the evidence of a criminal actions from a digital source. However, the varying range of data stored in digital devices can help with the investigation.

- Attribution

Logs from a computer and other metadata can be used to understand actions of an individual. For example, personal data residing on a computer drive can be used to identify its owner.

- Alibis and statements

Information provided by involved parties such as defendant or witnesses can be cross checked with digital evidence. For example, When mobile phone records of the person the perpetrator claimed to be out of town at the time were reviewed during the inquiry into Amit's murder The alibi was later discovered to be falsified.

- Intent

Cyber Forensics not only help us to find evidence of a crime being committed, but investigations can also be used to prove the intent of the criminal. For example, the Internet history of convicted killer included references to a website discussing How to kill people.

- Evaluation of source

The origin of a specific piece of data can be determined using file meta-data. For instance, older versions of Microsoft Word included a Global Unique Identifier in their files that could be used to determine the computer on which the file was originally written. Proving if a file being examined was produced on the digital device or obtained from somewhere else which can be very important in the court proceedings.

- Document authentication

We also need to keep in mind meta data linked with digital documents can be easily modified (by changing the computer clock time you can change the creation date of a file or document). Document authentication depends on detecting and identifying this false information.

5.1 Network data reveals theft of trade secrets

Engineer Xiaolang Zhang worked for Apple's group that dealt with electric automatic vehicles. He had been working for the company for two and a half years when he made the announcement that he would be leaving and going back to China to care for his old mother. He disclosed to his management that he would be working for a Chinese maker of electric vehicles. The management was skeptical after the conversation. Company security opened an inquiry. The assessment of Zhang's network activities most frightened them after they had searched his two work phones and laptop. According to the network data, Zhang's activity peaked in the days before he resigned, reaching a two-year high. There were mass searches and selective downloading of many pages of data. extracted from password-protected databases that he had access to, Zhang acknowledged stealing company information when questioned. Zhang was charged with theft of trade secrets after the case was forwarded to the FBI.

A branch of digital forensics is network forensics. In order to trace or monitor network activity, it entails the examination of log data from servers and other networking appliances (such as firewalls, routers, and intrusion detection software). Network forensics is one of the go-to technologies for intrusion and breach detection, thus attorneys with cyber law practices have grown extremely familiar with it. Network forensics may entail ongoing traffic monitoring or retrospective analysis. Data analytics methods are widely employed since the amount of data collected can be very large.

Network forensics used to be a very uncommon practice. Only a small number of companies have their network logging functions enabled in order to minimize the demand for storage hardware. Even fewer still kept their logs long enough for investigators to find them useful. As businesses have gotten smarter and more vigilant about cyber security, practices have altered. The Zhang case highlights how the accessibility of network data creates options to look into user behavior in situations that are not cyber-related, such as a theft of trade secret issue. Network logs can be examined, just like in the Zhang case, to spot large-scale data

transfers or deletions as well as other questionable user behavior.

5.2 Wearable sensors revel data.

In 2015 the murder of Connie Dabate in her residence. Her husband Richard gave a detailed account of what happened that day, stating that he came home after getting a warning from an alarm, according to the arrest order for him. Richard continued by stating that he was tortured and rendered helpless by an intruder after entering his home. When Connie arrived home from the gym, the intruder shot and killed her. Police were able to demonstrate that Connie was present in the home during the time Richard claimed she was at the gym using data from Connie's Fitbit. The Fitbit's data showed that Connie stopped moving a minute before the home alarm sounded.

Wearable technology, such as Fitbits, uses GPS to track location as well as activities like step count, distance travelled, and sleep duration. The hardware is set up to synchronize data with cloud or social media services, as well as programs on cellphones and personal computers. Both of these sources can be used to create evidentiary collections utilizing common digital forensics tools and methods.

5.3 Data from vehicle infotainment system can be useful.

In a 2017 article from Digital Forensics Magazinex, a hit-and-run collision involving a black SUV with no lights on is described. After colliding with a vehicle and a group of trees, the SUV continued on its way. Police found a matching SUV to the description. Police were able to ascertain several things after downloading data from the SUV's on-board diagnostics, infotainment, and telematics systems, including that the SUV had passed the crash site at or near the time the crash had occurred, that the lights had not been on, and that it had been put in reverse and forward several times shortly after the crash in close proximity to the damaged trees. Police also discovered other evidence linking the SUV's journey.

As a source of data for investigations, cars are fast approaching the level of personal computers or cellphones. Additionally, some automobiles come with web browsers which store cookies, history, and cache data. Data from programs that are incorporated by the manufacturer, like Facebook, may also be included. It is possible to recognize gadgets that have been connected to a vehicle's computer, much like with personal computers. In the near future, it could also be feasible to retrieve video data and history from the autonomous driving technologies that are now appearing in automobiles.

A growing area of digital forensics expertise is vehicle forensics. The majority of the effort to date has been focused on a single forensic instrument, but the tool's creators assert that it is compatible with more than ten thousand other truck and car brands. Automobile manufacturers, auto insurance investigators, automobile rental businesses, police enforcement, and intelligence organizations are already active users of vehicle forensics.

6. CONCLUSION AND RECOMMENDATIONS

Businesses lose an estimated $100 billion a year due to corporate espionage: the theft of corporate secrets for profit. To make matters worse, the biggest risk to a company isn't from an outside entity–instead, it is internal parties who pose the greatest threat. Whether it's disgruntled employees, or those looking to make extra money selling trade secrets, corporate espionage is a serious issue for businesses. Fortunately, there are ways to mitigate the possibility of such an issue from occurring.

- Minimize and Safeguard Physical Documentation-

Mostly the reason of corporate espionage occurs through the theft of a physical document, hard disk, pen drive, SSD or other type of physical information, not through hacking. Due to this, it becomes very important to control and manage the levels of physical documentation that exist within a private company. Never simply throw away important documents–always shred them before disposal with a high quality, cross-cut paper shredder.

- Protect Digital Information-

Digital theft makes up one quarter of corporate espionage cases, so it is important to protect digital information by installing and regularly updating security programs and protocols. This may include firewalls, antivirus and anti-Trojan software. Only allow trusted IT specialists to access servers, and change passwords regularly to prevent them from being cracked. Besides sensitive information and proprietary knowledge, make sure that any electronically stored intellectual e-properties, such as patents, copyrights or trademarks, are protected as well.

- Screen Prospective Employees and Develop Non-Compete/Non-Disclosure Contracts-

Be thoughtful in your hiring practices, and perform background checks on employees who will be responsible for maintaining or accessing sensitive data. Maintain open lines of communication with employees, which may help you to detect disgruntled employees who would be willing to commit corporate espionage. Having employees sign a non-compete and non-disclosure contract may not prevent corporate espionage from occurring, but will give you strong recourse to seek action against an individual who commits an infraction.

- Rely on the Expert Knowledge of a Data Forensics Team-

You've worked hard to make your business what it is now, imagine all that hard work going to waste after a case of corporate espionage reveals all of your most lucrative and valuable secrets and proprietary knowledge. Do not let this happen to you enlist the assistance of Data Forensics, who can help to ensure your valuable information is protected. Our data security professionals can help train employees on data security and best practices for preventing corporate espionage, and, should the worst occur

ACKNOWLEDGEMENT

This Research is helpful for students who want to pursue a career in Computer Forensics, the research enlightens them on the practical application of computer forensics in legal proceedings.

REFERENCES

- Guide to Computer Forensics and Investigation, Bell Nelson, Amelia Phillips, Christopher Steuart 4th Edition Cengage Learning.
- Computer Forensics A Pocket Guide, Nathen Clarke, I.TG. vernance Publishing
- Computer Forensics: Computer Crime Scene Investigation, John R. Vacca 2nd Edition, Charles River Media.
- The Field Guide for Corporate Computer Investigations by Chad Steel
- www.securonix.com
- https://www.wrc.noaa.gov/wrso/security_guide.htm

BIOGRAPHIES

Prof. Mahesh R Kudalkar
M.Sc. Information Technology
Asst. Professor,
Mumbai