IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

Research Paper

CORPORATE ESPIONAGE

Namratha Sharma
Guest Faculty, Nizam College, Hyderabad, India.

Abstract
This paper highlights the various aspects of Corporate Espionage where numerous points come into light, which discuss where, why and how espionage takes place by various individuals with the use of several technologies coming up in the market to steal the sensitive information of competitor firms . This paper helps to understand different sides to safeguard a firm from corporate espionage and it also covers diverse real world examples of espionage taking place.

INTRODUCTION

The computer age has ushered in a number of paradigm shifts in science, technology and commerce. Innovations and techniques have made life easier but along with the boon come the bane. One of the most serious flaws emanating from the use of technology is that of corporate espionage, which is an activity involving secretly eliciting any kind of trade secrets of peers regarding their upcoming plans so as to make oneself ready to compete with them or to come out with the same plan before they do so, obviously, to gain competitive advantage. This is usually done by spying into the competitor's organisation, stealing or running a covert plan to obtain the company's vital information.

Corporate espionage is mostly a very nicely planned activity. A spy in many cases can be an insider, who is an employee who keeps on passing the trade secrets from the organisation. The main aim is to gain initial access to the data and later on, to obtain the advanced control with which they can have a continuous access to the peer's data. It can also be done by out rightly entering into the premises using forged ID cards usually after office hours and searching for the needed information in the computers, hardisks and paper works. There are serious consequences of indulging in such dangerous acts as there are chances of them getting caught. An example of corporate espionage is the recent petroleum ministry case. The act of espionage may not be an intentional one initially, as a disloyal employee, just for the sake of personal advantage can indulge in the act of espionage.

The scope of corporate espionage covers a number of areas such as new projects, client's lists, research data or new marketing strategies. The intentions of spying can differ from case to case, but usually it is done to get an upper hand over the competitor in the market. Leakage of information can be very critical and the repurcursions of such spying can have an adverse effect on the performance of the organisation. It can be so dangerous that as a result of espionage a company may have to see the worst phase in its run. The intentions can be so malicious that they can directly bring down the targeted revenue of a new launch by more than 50% which is a huge loss to the company which is deceived.

Espionage may not be an act of one single person, usually it involves two or more of them because such information is kept at very secret places and access to them is allowed only to restricted personnel.
Types of Information used in Corporate Espionage

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

OBJECTIVES OF THE STUDY

The objectives of the study are to

- Trace the origin and history of corporate espionage.
- Understand its nature and how it takes place.
- Analyse the techniques to safeguard the system through real world examples.
- Make suggestions and recommendations so as to minimise such heinous acts in future.

REVIEW OF LITERATURE

- Omid Nodoushani, Patricia A. Nodoushani- " This paper aims at defining various forms of industrial espionage in the light of the ongoing information technology revolution. In the Digital Age, industrial espionage remains the dark side of the post-industrial revolution. The Federal Industrial Espionage Act of 1996 aimed at leveling the field regarding widespread cheating and stealing of intellectual properties by competitors in the marketplace".

- Raymond Palmer,"BUSINESS ESPIONAGE is currently one of the most insidious threats facing successful British companies."

- Phillip C. Wright, Géraldine Roy, "This paper discusses the difference between industrial-espionage and competitive intelligence so that practicing managers will be more able to formulate policy in this critical area. As well, procedures for securing information as part of a competitive intelligence process are outlined."

- Bill Fiora, "Business intelligence is one of the fastest growing disciplines in corporate America. To many, however, the words conjure up images of trench coats and meetings in back alleys. Unfortunately, recent

events serve to reinforce these fears like, Volkswagen agreed to pay $100 million to General Motors after the U.S. firm alleged that VW used documents pilfered by an ex-GM executive to its competitive advantage., Johnson & Johnson and Boehringer Mannheim settled out of court after trading accusations of improper activities, including infiltrating company meetings and taking confidential documents. Even more unsettling to some may be the passage of the Economic Espionage Act in 1996."

TYPES OF CORPORATE ESPIONAGE

- **Human resource**: Stealing the information by means, which directly involve human activities like spying, unauthorised entry into the premises, bribing employees.

- ***Kodak Vs Harold Worden***
- Pensioner power was something that Harold C. Worden obviously believed in. After completing 30 years with the Eastman Kodak Corporation he retired and promptly set up a consulting company, brokering the services of over 60 other retired Kodak employees. In his last five years working for Kodak, Worden was intimately involved with the development of the 401 film machine.
- Not content with simply bringing with him several thousand confidential documents relating to the machine, he also convinced his successor to provide him with even more. He was sentenced to one year in prison and fined $30,000, only a little more than he had received for the stolen information, which Kodak held to be worth millions of dollars. One wonders whether Worden pawned his gold watch too…

Source:http://www.businesspundit.com/10-most-notorious-acts-of-corporate-espionage/

- **Wiretapping**: Tracking and monitoring the traffic on internet and recording telephone lines by covert means is called as wiretapping or telephone tapping. It can be done by any third party or by one of the parties involved in the conversation without the knowledge of other party involved in the conversation. Tapping can be done either by recording the conversation on tapes or by actively listening to the conversation. Mobile phone tapping can also be done by remotely activating their microphones of the mobile and listening to the conversation of the people around the person who is holding phone. Tapping is majorly done by government agencies to gather information and make themselves ready for any upcoming threats and is called lawful interception which is very different from what we see in espionage because it is illegal in the later.

- **Secondary's Torage Devices**: To copy data from a computer one needs a secondary storage device like CDs,SD card,Pendrives etc. Copying information to these devices does not leave any prima facie evidence that there has been any transfer of data. In the current scenario we see that due to security reasons companies do not allow such devices in to the office premise but Inspite of such restrictions people are able to carry them in the offices and copy the needed information and this is because of disguised looks of pen drives and SD cards. Now days we find in market pen drives in different shapes few look like key chains or concealed ones which look like a wristband or like a ball.

- **Hacking**: One of the top three methods for obtaining trade secrets which is increasingly getting popular is Hacking, the reason being the easy availability of such tools over internet and such tools can be easily used by any person as they do not require any in depth knowledge about any protocols or codes.Hacking can be categorised into three types: System hacking, Remote hacking and Physical hacking
    - In **System hacking** the person already has access to at least a low level profile and if the security systems are not up to the mark then he can have a good chance to hack information of a high level profile.
    - **General Motors v/s Volkswagen In** 1993, General Motors accused Volkswagen of industrial espionage after Jose Ignacio Lopez, the chief of production for GM's Opel division, left to join the rival German automaker, along with seven other executives. GM claimed its corporate secrets were used at VW. In the end, the companies agreed to one of the largest settlements of its kind:

GM would drop its lawsuits in exchange for VW's pledge to buy $1 billion of GM parts over seven years. In addition, VW was to pay GM $100 million.
Source:http://www.bloomberg.com/bw/slideshows/20110919/famous-cases-of-corporate-espionage

- In **remote hacking** the attacker tries to access the information by penetrating the system using internet or intranet. Once the attacker is able to penetrate the system then he can have access to all the high level information and will be able to provide access to others also and if he is able to hack the security system of the organisation the he can allow any unauthrised person to enter the premises and also restricted areas where only key personnels are allowed to access.

❖ **McAfee v/s Dell SecureWorks** In what was described as one of the largest cyberattacks, more than 70 companies, governments, and nonprofit organizations were hacked by spies beginning in 2006, according to security company McAfee, which didn't name the perpetrator in its report. Dell SecureWorks, another security company, traced the same attacks and pointed to China as the source of the attacks. Victims included a U.S. real estate company, a New York media organization, defense contractors, a South Korean steel and construction company, the International Olympic Committee, and the World Anti-Doping Agency. Hackers took information from some of the victims over a period as long as two years.

❖ **Gillette v/s Steven Louis Davis**

In 1997, an engineer who worked with Gillette to help develop its next generation shaver system disclosed confidential information to the company's competitors. Steven Louis Davis, an employee at Wright Industries Inc., a designer of fabrication equipment that was hired by Gillette, faxed or e-mailed drawings of the new razor design to Warner-Lambert, Bic, and American Safety Razor. Davis pled guilty to theft of trade secrets and wire fraud and was sentenced to 27 months in prison. He told the court he stole the information out of anger at his supervisor and fear for his job. Photograph

Source:http://www.bloomberg.com/bw/slideshows/20110919/famous-cases-of-corporate-espionage.

- **Physical hacking** is where a person himself enters into the facility and once he is in then he can roam around looking for a vacant and open computer with employee's login and password lying around. The attacker can come across letter heads and then can upload fake circulars or documents into the private network. He can further have access to paper work which can consist the important contact numbers. He can also manipulate the data which may give undesired results.

THE WHY OF CORPORATE ESPIONAGE

It can be seen that corporate espionage has become a corporate evil and a menace. Eroding values across society and cultures have given way to easy and loose morals. Cut throat competition and the cat kill dog mentality has led companies to stoop to such base acts vigorously, by hook or by crook. Competing companies always keeps an eye on their competitors to seek information regarding their company's moves, their target is seeking various information like the various Corporate strategies in Product designing, Manufacturing, Research, Costs and Technological Operations, various development in industries like Plant closures and development, business methods, contract arrangements and Alliance like delivery, pricing. Marketing, advertising and packaging expenditures, details such as Customer and supplier details, Staffing, Operations, Organisation Charts, Wage/Salaries. Apart from this, personal information is also targeted such as Residential addresses, contact number, Names of spouse, children details, salary, Medical records. Credit records or credit union account information and Performance reviews.

❖ ***IBM Vs Hitachi***

This case of computer company corporate espionage was dubbed "Japscam" by the press – perchance in hopes of a made for TV movie or perhaps a computer game! In 1981 Hitachi mysteriously came into possession of an almost full set of IBM's Adirondack Workbooks. It seems that the fact that they contained

IBM design documents full of IBM technical secrets and were prominently marked FOR INTERNAL IBM USE ONLY didn't prompt Hitachi to return them.
IBM counterintelligence staff and FBI personnel worked tirelessly until the arrest of several IBM officials proved the fruits of their labor. Hitachi settled out of court, and paid IBM a sum that has been reported as US$300 million.

Source:http://www.businesspundit.com/10-most-notorious-acts-of-corporate-espionage/

ANALYSING TECHINIQUES TO SAFEGUARD THE SYSTEM

Companies at various levels hold advantages which sometimes turn into disadvantage for an organisation. Espionage is a lever of threat where companies unfortunately loose its trade secrets and technology. To safeguard these companies, it is imperative or them to adopt various strategies to reduce the risk of corporate espionage. They are:

- **Identify cyber trade hush-hush and ensure security**
  The most important aspect is to identify whether a company is holding trade secrets or not, if yes then seek ways to keep them fool proof against spying through acts of Copying, recording, transmitting and accessing of important files.

- **Identify threats and ensure physical security**
  It is very crucial to identify a company's threat. For instance, it can be said that competitors pose to be dangerous; as a result a company should be vary of and be alert with its visitors, co-partners, consumers, hackers and even national foreign government can be a potential threat and should be considered a counter espionage plan. Firms should be provided with the perfect security and should be kept under surveillance. A physical security should be provided in the office, infrastructure and with the equipment. Firm should also be careful with the entry and exit points and even at hiring contractual personnel.

- **Establish policies for controlling information**
  The flow of information has a great impact on an organisation, as the information gets disclosed to all the employees at various levels, where the employees should have a clear idea of which information is to be shared within the organisation and which can be leaked outside. There should be a proper control on storage and retrieval of data. Particular attention should be paid to what is disseminated over the Internet and social media sites. Additionally, firms should develop procedures for the proper disposal of paper documents, IT hardware, and other sensitive equipment.

- **Train the Workforce and provide Compartmentalized Information**
  The organisation should look after the proper training of human resource so as to follow a systematic procedure for their induction. Industrial threats and securities should be taken care off so as to identiy and report any suspicous activity found to the required authority. Restricted and confidential information should not be made accessible to all employees but only to those for whom it is meant to be and who can be trusted and loyal to the organisation.

- **Conduct employee backgroung check and exit procedure**
  A firm shold make an effort to identify all possible factors which makes as employee prone to illegally disclosing information by conducting various background checks of the employees and should monitor things by keeping a regular eye on activities like security evaluaton. The employee entry and exit should be controlled with high security, as it is important to make employee exit as smooth and resentment free.

CONCLUSIONS

Corporate espionage has emerged as a burning topic. Articles have appeared in print and on the internet; movies too give an insight on the need for curbing such illegal practice. Different cases on spying in the offices to gain a competitive advantage have been reported but more research has to be done on such issues but this will depend on

companies steering clear and providing information on the misdeeds of its employess, but the question is will they disclose such instances and provide relevant information as and when required is the million dollar question.

REFERENCES

1. Omid Nodoushani, Patricia A. Nodoushani, (2002) "INDUSTRIAL ESPIONAGE: THE DARK SIDE OF THE “DIGITAL AGE”", Competitiveness Review: An International Business Journal, Vol. 12 Iss: 2, pp.96 – 101
2. Raymond Palmer, (1974) "Espionage threat to British industry: Spies don't only operate in books and films. They can be for real. And their target might be your industrial secrets", Industrial Management, Vol. 74 Iss: 7/8, pp.10 – 13
3. Phillip C. Wright, Géraldine Roy, (1999) "Industrial espionage and competitive intelligence: one you do; one you do not", Journal of Workplace Learning, Vol. 11 Iss: 2, pp.53 – 59
4. Bill Fiora, (1998) "Ethical business intelligence is NOT Mission Impossible", Strategy & Leadership, Vol. 26 Iss: 1, pp.40 – 41
5. Source:http://www.businesspundit.com/10-most-notorious-acts-of-corporate-espionage/
6. Source:http://www.bloomberg.com/bw/slideshows/20110919/famous-cases-of- corporate-espionage