Educational Administration: Theory and Practice
2024, 30(6), 548 - 552
ISSN: 2148-2403
https://kuey.net/

Research Article

Stealing the edge: How corporate espionage threatens India's growth

Ms. Snigdha Bishwal[1*], Ms. Sivashrita Bharadwaj[2]

[1*]Assistant Professor of Law, SOA National Institute of Law, SOA University, Bhubaneswar, Odisha. Email - snigdhabishwalo@gmail.com
[2]Assistant Professor of Law, SOA National Institute of Law, SOA University, Bhubaneswar, Odisha.
Email - sivashritab@gmail.com

Citation: Ms. Snigdha Bishwal, Ms. Sivashrita Bharadwaj, (2024) Stealing the edge: How corporate espionage threatens India's growth, Educational Administration: Theory and Practice, 30(6), 548 - 552
Doi: 10.53555/kuey.v30i6.5260

ARTICLE INFO

ABSTRACT

Cyber security is a significant concern for organizations and the top priority for corporation and its leaders has become the protection of information assets. However, due to lack of a proper legislation and inadequate cloud computing strategies of big organizations, the risk pertaining to data privacy and security could possibly increase in India. Competitive Intelligence being a legal and ethical concept is just the exact opposite of Corporate Espionage. The internet has brought forth considerable improvisations in collecting information and data related to anything and anyone. Spies are no longer required to physically break into offices or homes to get hold of sensitive information. While being indulged in the acts of Corporate Espionage, the internet and techniques used are equipped with more advanced 'attacking' mode. Cyber-attacks at present are becoming increasingly usual in both public and private areas with systematically organized criminal groups who are offering to conduct intricate and complex hacks to espionage sensitive information of rival corporations. Thus, all this threats and menaces call for a robust and stringent laws pertaining to cyber offenses This paper essentially discusses the threat imposed by cyber-crime upon sensitive information held by the corporations and the need for policy and legislation to mitigate the ill-effects of it.

Keywords: Corporations, Data protection, Espionage, Cyber crime, Cyber security

INTRODUCTION

"Whether an infiltration is criminally or politically motivated, a cyber-attack can have a negative impact on a company's value, reputation and ability to generate revenue."
-Sivarama Krishnan, Executive Director, PwC, India

With increasing competition and economic pressure coupled with development of new platforms for technology, companies are using ethical but mostly unethical means to substantiate their brand, launch new products, retain the best employees and acquire sensitive information of competitors, thereby saving money and increasing profits from losses to competitors. Parallel to this, there exists an increasing threat of cyber-attacks which has put investors, senior executives, and policy setters under much pressure. Consequently, corporate espionage has undergone a paradigm transformation as more effective and subtle ways of espionage have developed. The internet has proved to be a 'highway of information' for obtaining knowledge related to anything or anyone and its unethical use in corporate espionage raises alarming law enforcement concerns.

Corporate Espionage lacks a codified definition, but it is simply, "corporate practices wherein a corporate organization or structure with the help of spies or advanced technological systems facilitates the leakage of confidential information which could impact the general growth of the victim or usually a rival organization. Trade Secrets of a corporation which includes intellectual property (IP) (electronic communications and files), R&D reports, large databases, market strategies, etc. are some aspects of any organization that are nder severe threat.. Several sectors such as IT-BPO industry, infrastructure, FMCG, banking, insurance,

manufacturing, telecom sector and most importantly electronics and infrastructure are most vulnerable to corporate espionage.

In **United States v. Steven Louis Davis**, David was accused of disclosing trade secrets of Gillette Company concerning a new shaving system developed by the same and was sentenced to two years and three months in federal prison.

In 2013 customer data of a private insurance company was stolen by a rival company thereby violating the Information and Technology Act and section 379 of the Indian Penal Code for committing theft of customer data.

It's almost impossible to measure or estimate the actual or potential losses of corporate espionage since in terms of effect, a stolen ad campaign or a stolen design is not easily measurable and the threat has mushroomed under the added component of cybercrime. Moreover, internet has developed 'Espionage as a Service' (EaaS) as the largest threat to the biz-world as the cyber criminals have started to realise that the right piece of information can be more lucrative business deal than stealing hefty amounts of cash and moreover, data can easily be sold on the internet in an anonymous manner. Groups selling EaaS include low-level hackers, Organized Criminal Gangs (OCGs) that try to enter corporate websites through plugins by experimenting with complex and high level techniques aimed at the big industries such as defence, IT, legal firms involved in M&A and patent law, etc.

In United States the Economic Espionage Act, 1996 (EEA) addresses theft of trade secrets. The EEA criminalizes the theft or misappropriation of trade secrets. One provision is focused on foreign economic espionage which requires that the theft of the trade secret be done to benefit a foreign government, instrumentality or agent. The other provision relates to more common commercial theft of trade secrets, regardless of who benefits.

In India the Information Technology Act, 2000, Indian Penal Code, 1860 and principles of contract law provide legal protection to transactions carried out by means of electronic data interchange and other means of electronic communication. The Information Technology (Amendment) Act, 2008 contains a new provision in the form of S. 43A relating to data protection, privacy, cyber terrorism etc. It protects sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource owned, controlled or operated by it. "If such a body corporate is negligent in implementing reasonable security practices and it causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected."

LEGAL FRAMEWORK FOR REGULATING CORPORATE ESPIONAGE AS AN INTERNET FRAUD

Corporate Espionage in the United States is essentially regulated by two formal legislations. There is specific law for the protection of trade secrets called the Uniform Trade Secrets Act published by Uniform Law Commission 1979 and amended in 1985, and in addition, Economic Espionage Act, 1996 (EEA) regulates the corporate crime of Espionage.

The EEA contains two separate provisions that criminalize the theft or misappropriation of trade secrets. The first provision is directed towards foreign economic espionage and requires that the theft of the trade secret be done to benefit a foreign government, instrumentality or agent. The second provision makes the more common commercial theft of trade secrets, regardless of who benefits a criminal offence.

No separate law in India for protection of trade secrets

In India, there is no specific law for the protection of trade secrets. However, The 22nd Law commission has recommended for the introduction of new legislations related to the protection of trade secrets and also on economic espinage. Therefore, for protecting trade secrets reliance has to be placed on Indian Contract Act, as well as under provisions of criminal law, or other equitable doctrines of breach of confidentiality. Normally, employees are restricted by the employers from divulging confidential information or trade secrets by inserting a "non-disclosure" or "confidentiality" clauses in the employment agreement. Indian Courts have mostly placed reliance on **Saltman Engineering v. Campbell Engineering Co. Ltd.** It was held in this case trade secrets that are disclosed in breach of confidential relationship will have protection of principle of equity. The information divulged must necessarily have the element of confidentiality and the obligation of non-disclosure continues till the time information remains confidential.

In the absence of any separate law on trade secrets, reference will have to be made to the definition laid down by the courts in India so as to guarantee protection to "trade secret" from being stolen. In the case of **Ambience India Pvt. Ltd. v. Shri Naveen Jain**, the Court observed that "a trade secret can be a formula, technical know-how or a peculiar mode or method of business adopted by an employer which is unknown to others." But, those information which are commonly in the knowledge of employees and his competitors is not considered as trade secret because already there in public domain.

Moreover, the Courts have laid down three situations in which proceedings for theft of trade secret may arise:

I.Where such fact of information that is secret has come in the possession of an employee in the normal course of his work, who passes that deliberately or carelessly, passes that fact or the information to an unauthorized person;

II. Where such an employee who is claimed to be in possession of such trade secrets has been invited to provide such information by such an unauthorized person.

III. Where, in the case of a license, the licensee has committed a breach of any condition that was expressly or impliedly given in the agreement.

In many cases, the Indian courts have held that "although an employer cannot restrain his employee from offering competition after he is terminated from the company, but, the employer has the right to reasonably protect his trade secrets against exploitation." In cases where the contract for such trade secret is absent, injunctions have been issued by the courts based on the rules of equity.

INFORMATION TECHNOLOGY ACT, 2000: LEGAL MEANS FOR REGULATION OF CORPORATE ESPIONAGE IN INDIA

Information Technology Act, 2000 (IT Act) is enacted for the recognition of transactions taking place by interchange of electronic data and mechanisms adopted in electronic communication. It provides safeguards with regard to privacy of information, protection of data, cyber terrorism etc. Chapter IX of the IT Act specifically deals with cybercrimes and provides for adjudication, compensation and penalties for committing cybercrime. Corporate Espionage being one of the most occurring cybercrimes in India is essentially regulated by the provisions of chapter IX.

Section 43 deals with cyber contraventions related to unauthorised access to computer, computer system, computer network or resources. It imposes a penalty not exceeding one crore rupees for downloading without taking consent, introducing any computer contaminant or computer virus into any computer, computer system or computer network. Section 66 provides punishment for the wrongful acts committed dishonestly or fradulently under Section 43 and imposes imprisonment for a term which upto three years or fie upto Rs five lakhs or with both.

Moreover, IT Amendment Act, 2008 inserted a provision that "any a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected." There is no limit on the amount of compensation that can be claimed by the person affected in such circumstances. It must be noted that no definition of "sensitive personal data" has been provided in the Act.

Section 72 provides for the breach of privacy and confidentiality. It mentions that any person who has a secured access to any electronic record book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such material to any other person would invite punishment with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both. As per section 72A of the IT Act, knowingly and intentionally making disclosure of information without the consent of the concerned person and in breach of the contract is punishable for period up to three years and fine which may extend up to Rs. 5 lakhs.

JUDGMENTS PRONOUNCED ON CORPORATE ESPIONAGE

1. A leading multinational conglomerate company levelled corporate espionage

In 2012, a leading MNC levelled espionage charges against an employee of another conglomerate for stealing a particularly sensitive display technology used in smartphones and other mobile devices. Samsung demanded the accused firm to make a public apology and also pay a fine of roughly about 10,000 USD and ensure that it will not steal engineers moving forward. The accused has on return filed a suit alleging defamation. Six employees of the accused are expected to be involved in this. The judgement is still awaited.

2. Ford's trade secret theft case

Xiang Dong Yu, a former product engineer for the Ford Motor Company for almost a decade, had access to Ford's trade secrets. He copied 4,000 Ford documents onto an external hard drive and returned back to China with that hard drive. Those documents include sensitive Ford design documents such as system design specifications for the Engine/Transmission Mounting Subsystem, Electrical Distribution System, Electric Power Supply, Electrical Subsystem and Generic Body Module. Ford valued the loss of the trade secrets at $50 million dollars. In April 2011, Yu Xiang Dong was sentenced to 70 months in federal prison for theft of trade secrets and economic espionage.

3. Stealing of Goldman Sachs Computer Code

Sergey Aleynikov, a former employee at Goldman Sachs, was delegated with the responsibility of developing computer programs. On June 5, 2009 i.e., his last day working at Goldman Sachs— He transferred substantial portions of the firm's proprietary computer code for its trading platform to an outside computer

server in Germany. After transferring the files, he removed the program which he used to encrypt those files and deleted his computer's log. On top that, during the course of his employment as well at Goldman Sachs, he transferred thousands of computer code files related to the firm's proprietary trading program from the firm's computers to his home computers, without the knowledge or authorization of Employer Company. Later on, he was sentenced in Manhattan federal court to 97 months of prison for stealing valuable, proprietary computer code of Goldman Sachs.

4. Trojan Horse Case

Two people from London, Michael and Ruth Haephrati came up with an idea of a Trojan horse program that was originally invented with an intention of spying on Michael's ex-wife's computer. However, the Haephrati came across the grandeur uses of the said virus. He tried marketing it to Israel's defence agencies before Michael could decide to sell it to private investigators representing corporations. Subsequently, the said Trojan horse was used by a major Israeli corporation to infiltrate and spy on its competitor and its subsidiaries.

5. Sharing Trade Secrets with Rival

A Net gear engineer/product development manager with the help of an extranet connection downloaded multiple files relating to trade secret from Marvell Semiconductor, a business customer of Net gear itself. The said engineer accepted the employment with and then 'allegedly' shared the Marvell files with the rival employees.

ANALYSIS AND SUGGESTIONS

In order to protect each company from the corporate espionage the following suggestions might be helpful in escaping the danger of data tumbling into the database of the competitors.

1. Information must be classified into sensitive and important information. The easy catch is innovative processes or market strategies. The usually unprotected information is customer lists and files of the personnel.
2. In order to identify the vulnerable information, a risk assessment must be done by the companies.
3. After identification of vulnerable information, updated security policies must be adopted in order to safeguard the data of the company.
4. Every employee must be trained irrespective of them belonging to the IT department. They must be trained to identify the valuable information and what procedures must be adopted to protect them. In case of suspicion of solicitation of information to competitors, strict action must be taken against such personnel.

CONCLUSION

India is slowly moving forward and has taken a great leap towards reducing cybercrimes through the IT (Amendment) Act, 2008. It is evident from the above that new developments in technology and internet demands strict laws for theft of confidential information or competitively sensitive information. Every company today is facing the unseen challenge of technological development advancing through our lives. This clearly brings out the requirement of a strict and efficacious cyber security law. There needs to be a common law or set of common rules for all countries as due to such gap between uniformity of rules, it becomes easy for the spies to break into computer networks. Every company must adopt an ethical code of conduct in their business. Moreover, a proper and efficient trade secret law will hold all businessmen and companies accountable and responsible. Adoption of a separate trade secret protection will bring clarity in foreign investors and reach heights in business acumen.

Indeed knowledge is power. The more knowledge corporations have about the threats that are out there, the better they will be able to defend themselves from attempts to steal their jackpot.

REFERENCES

1. SHANE W ROBINSON, Corporate Espionage 201, SANS Institute IndoSec Reading Room, 2007, Pp. 3; Available at: https://www.sans.org/reading-room/whitepapers/engineering/corporate-espionage-201-512
2. HARSH SINHA, Corporate Espionage and the Information Technology (Amendment) Act, 2008, Volume 3 – Issue 2, Indian Law Journal (2007); Available at : http://www.indialawjournal. org/archives /volume3/issue_2/article_by_harsh.html
3. PricewaterhouseCoopers Publications, Invading Privacy : Cyber Crimes on the rise, 2013; Available at : https://www.pwc.in/assets/pdfs/publications/2013/invading-privacy-cyber-crimes-on-the-rise.pdf
4. STUART POOLE-ROBB, Corporate espionage – the internet's new growth industry, IT Pro Portal (2015); Available at : https://www.itproportal.com/2015/03/19/corporate-espionage-internets-new-growth- industry/

5. ZAFAR MAHFOOD RAHMANI & FAIZANUR RAHMAN, *Intellection of Trade Secret and Innovation Laws in India*, 16(4) J. Intell. Prop. Rts. 341, 347 (July 2011)
6. VIJAY PAL DALMIA, Data protection Laws in India, available at: http://www. mondaq.com /india/x/133160/Privacy/Data+Protection+Laws+In+India
7. PriceWaterhouseCoopers Publications, Invading Privacy : Cyber Crimes on the rise, 2013; Available at : https://www.pwc.in/assets/pdfs/publications/2013/invading-privacy-cyber-crimes-on-the-rise.pdf
8. Reuters, "Israel holds couple in corporate espionage case." As on January 31, 2006, available at http://news.zdnet.com/2100-1009_22-6033129.html
9. ORSBERG, BIRGITTA, "The spies in the next cube Silicon Valley a magnet for trade secret theft -- and it's often an inside job." San Francisco Chronicle, as on April 25, 2005, available at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/25/BUGGLCDPUJ1.DTL