A Literature Review:
Industrial Espionage

Harrison John Bhatti & Andrii Alymenko
Master's Programme in Industrial Management and Innovation
School of Business and Engineering
Halmstad University, Sweden.

Emails: harbha16@student.hh.se; andaly16@student.hh.se

Abstract

This is a literature review article. The purpose of this article is to explain and provide a deeper understanding of economic and industrial espionage. Furthermore, it describes legal and illegal methods of espionage and highlights the different aspects of preventing espionage such as: technical, operational, physical and personnel security. A number of theoretical concepts have been extracted and analyzed from different scientific articles which have been summarized and anticipated in the form of theoretical framework. Incredible results are often produced by exploiting industrial espionage. By concentrating on complete security, and not simply specialized security, data security experts can altogether hamper enemy endeavors to take their association's data resources.

Keywords: *Industrial Espionage, Economic Espionage. Corporate Crime, Espionage Methods, Avoiding Espionage.*

1. Introduction

One of the issues for the confrontations within the field of data security is the scarcity of tenable knowledge about existing threats to intelligence protection. Governments and companies experience a deficiency of ascertainment and information gathering in this field and face an increasing problem of industrial espionage (Thorleuchter & Van den Poel, 2013). Moreover, different researchers such as: Malone, Baluja, Costanzo, and Davis (2000) show the evidence that many of the recognized intrusions in the information systems are ignored which makes impossible to provide the proper statistical analysis. However, in many cases described by Polanyi (1967) theft of knowledge from the organization is not allowing robbers to use the technology and results in further violations such as luring away employees or even kidnapping.

Humanity knows a variety of industrial espionage examples as well as preventive methods through the history. Thus, Britain's patent laws of the 1780s aimed to prevent stealing technologies in emerging textile industry (Ferdinand & Simm, 2007). During American Civil War, as shown in Mendell (2011) work, Mrs. E.H. Baker was memorizing the firepower layout and technologies of Confederate States' submarines and transmitted the information to the South States' Navy. Herring (1992), draws the great example of intelligence gathering which

later helped to build one of the most powerful financial empires from North of Europe. With the help of one of his employees, the Swedish banker Marcus Wallenberg has managed to copy the idea of intelligence cooperation between the French government and local banks.

Data security experts center their endeavors on what they know best. Technical security systems have a high level of impact on the intelligence protection. Thus, the most part of the budget for the protection from espionage is spent on Firewalls and Internet security software enabling the safety from hacker attacks. However, the attention focus on the protection from the external intrusion does not save organizations from threats from insiders which are responsible for more than 70% of thefts related to information systems (Pitts, 2008). Moreover, the focused hacker attack can dodge most of the electronic protective mechanisms, which often demonstrates the waste of budget on inefficient software.

From the above statements is clear that the information has different forms. The task for the information security professionals is to assure the maximum protection in these forms: operational, technical, physical security and prevention of personnel information outflow. The weak gap in any of elements of the protection system will give the advantage for the industrial spies to sneak in and steal the data.

2. Literature Review

2.1 Economic and Industrial Espionage

Different scholars give various definition and names to industrial espionage. Wright and Roy (1999), name it as corporate or economic espionage and industrial intelligence. Søilen (2016) distinguish economic and industrial espionage explaining that the last one is exempted from the involvement of the government in collecting information and stealing the knowledge. Per se, military use a version of economic espionage as warfare through the internet to destroy the core infrastructure of the enemy's country. Nasheri (2005), explains the strategic connections between government intelligence outfits and the success of taken nation. The first shifts in industrial espionage methods started along with the existence of the information age and World Globalization. The US Economic Espionage Act outlines the legal aspects of industrial espionage leaving open the discussion either to keep trade secrets or move forward the open global society.

The current literature explains the thread caused by the industrial spies. According to I. Winkler (1997), vulnerability aspects of the organization must be analyzed comprehensively in order to reduce risks from the various channels of information attacks from industrial spies. Cornwall (1991) gives the emphasis on the explanation of methods and techniques for the practical approach of collecting intelligence from companies in a 'civilized' way. On the contrary to Cornwall, there are researchers including Rustmann (2002) who describe the industrial espionage as a cynical target-oriented business giving the bright examples of the non-ethical CIA operations.

Penenberg and Barry (2008) give comprehensive details of the relations within spy organizations who provide the industrial spies for the governments. The vulnerability of

certain entrepreneurs plays an important role in the success of industrial espionage. However, Perman (2010) indicates the high importance of the professionalism of spies, giving the example of the commercial success in technological start-ups after applying the espionage techniques of Israeli militarists. Mendell (2011) drives the focus to the espionage attacks risk reducing describing practical ways of security operations. Furthermore, he develops and the idea of 'internal intelligence' for the surveillance and control of employees and activities within the company.

2.2 Corporate Crime

Corporations are valuable business units which have a high scope of the economic and political influence on the society. Some cases of corporate criminal activities appear within the 'white-collar' community and not always are of the economic nature. According to Pontell and Geis (2007), the positional power and the corporate culture are the main drivers for the white-collar criminal behavior of individuals. The main reasons for the criminal engagement of the individuals through the corporate mechanisms are apparent awareness (or unawareness) of the criminal activity results or the collective misinterpretation of the truth within the whole value chain activities.

Hence, the statement above shows the evidence that behavioral habits in the organization may contribute to the choice-making decisions towards corporate criminal activities. Nasheri (2005, p. 7) gives two possible scenarios for the employees' crime activities in a corporation: in one case dissatisfaction of the job pushes people to use the information secrets of the company for their own benefits; in another case, external actor (competitor or foreign nation) misappropriates the trade secrets from organization or another nation. Michalowski and Kramer (2006) describe the mechanisms of the corporate crime and argue that most capitalistic nations commit regulatory crime established by its elite as a less crime than a street robbery. Having economic and political power these leaders can avoid the prosecution and reduce the risk of being convicted as crime acting individuals.

2.3 Methods of Industrial Espionage

There are materials in evidence of the actions of former Soviet agents for the industrial espionage as well as small groups of spy agencies hired by countries governments to create the thread in different nations' economies (Pasternak & Witkin, 1996). In many cases, the methods applied by these professional spies can break any protection in the companies' intelligence system.

2.3.1 Legal Methods

There are a few types of legal industrial espionage. Competitors can buy products from the company, as such, get the prototype or a working technology to explore. Buying a company is another legal method for acquiring the core technology. This method is widely practiced in the Global World Economy and none of the management can create the protection and prevent capturing the information in this case (House, 1995).

In the case of the company's willingness to enter the foreign market, it is possible to use another method of acquiring legal information: the company can be pressurized by the government or the partner of the foreign company to train the local workers and managers in the critical technology. The corporate security managers are not always involved in a decision-making process of entering the market and the senior management decides if the 'game is worth the candle' (House, 1995).

Industrial competitors are often able to gather the valuable information through the open source information (OSI). The thorough review of the newspapers, scientific articles, annual reports, patent filings, marketing materials, advertisements, apps, word of mouth etc. can give a wealth of knowledge about the company and its products. Very often the company could not realize the value of the information that is given away to the open source (House, 1995).

2.3.1 Illegal Methods

In many cases, the value of the desire to get the information pushes rivals to steal or copy it without permission. Very often the insiders are used to access the company. Traditionally, moles or someone with the good contacts in the company and willing to coop with criminals. These people often have the access to the necessary information or can provide the access for the spies in exchange for the money. In some cases, employees could be initiators for the information crime themselves, offering the corporate secrets to the competitors for sale (Pasternak & Witkin, 1996).
While traveling on the business trip, employees of the company can become a subject of sophisticated spy methods. Special monitoring devices, hidden cameras, and bugs can collect the necessary details about the company. Executives of the big US companies have reported commonly of search in their hotel rooms (House, 1995).

The methods of industrial espionage are limited only by the imagination of the spies. However, physical stealing of information is very effective and may give to robbers' information, which they would not collect in another way. It could be made by breaking into buildings and offices, connecting to the cables, downloading the files on the flash drive or a disk. Spies can also use the trash-diving to the garbage containers to gather the information. Very often it gives more information to the rivals than the person who unconsciously throws the documents to the trash bin may think.

2.4 Ways of Avoiding Industrial Espionage

The methods used in industrial espionage are similar to techniques of traditional spies. This gives the guidance for the companies which want to prevent stealing the information from their archives (House, 1995). As for big corporations, the potential loss of information counts in numbers of many figures, the preventive methods must, therefore, supply the proper protection and extensive countermeasures. These methods include physical, technical, operational and personnel security.

2.4.1 Technical Security

The implementation of technical protection provides electronic systems security. These countermeasures ensure the proper work of confidential standards of the company with integration into a computer network. All these technical methods are well known and work successfully within the electronic systems of many organizations (I. S. Winkler, 1996).

2.4.2 Operational Security

Operational security is based on the business model of the company or the value chain activities of the organization. The strict procedures of the transition and control of the information must be supported by the clear understanding of the marketing processes, research activities, product development, manufacturing, and distribution. The compromised information must be secured with additional control (I. S. Winkler, 1996).

2.4.3 Physical Security

As mentioned above, the threat of physical stealing of the information is a serious issue. Hence, the access to the company's facilities and archives must be strictly controlled and regulated. It can be ensured by the limitation of access for third parties, such as clients or partners and the employees. The organization should avoid the free access to corporate facilities, especially the archives with the critical information. If the company is big, it is a good idea to require all the employees to wear the corporate badges with a status indication (employee, visitor, partner etc.). This will avoid the awkward moments and the mock competence by violators. Moreover, the policy of the company should encourage people to check the badges of the individuals who they are not familiar with. Not the last issue to name is control of the trash which comes out the office to avoid the outflow of the information through the garbage disposal system (I. S. Winkler, 1996).

2.4.4 Personnel Security

All employees with the potential access to the important files should be carefully investigated for their background. It is good to have an electronic system access to the facilities, where everyone who enters the office uses an electronic ID to open doors or copy the data. The company should support the intercommunication of administrative and human resources departments. All unusual activities should be analyzed and investigated as soon as possible (I. S. Winkler, 1996).

3. Methods

This is a narrative literature review article where the observation strategy has been adopted in terms of conducting research for this paper. The data has been gathered by reviewing and analyzing of different literature reviews and published scientific articles. In terms of gathering and evaluating of different theories high ranking journals and databases such as Scopus, Web of Science, Science Direct, Emerald, Springer and Google Scholar have been used. The keywords that were used to find the relevant articles are: Industrial espionage, Economic

espionage, Corporate crime and in some cases some specific keywords were used to refine the search results.

The below table shows the databases, search words and the type of documents that have been used to analyze and evaluate different theories in this paper.

Table 1. Shows the Search Result of Articles

Databases	Search Word	Document Type
Scopus	Industrial Espionage, Economic Espionage	Article
Web of Science	Industrial Espionage, Economic Espionage	Article
Science Direct	Industrial Espionage, Economic Espionage	Article
Emerald	Industrial Espionage, Economic Espionage	Article
Springer	Corporate Crime	Article
Google Scholar	Industrial Espionage, Economic Espionage	Article

Cronin, Ryan, and Coughlan (2008) justify the research method and describes that Meta-amalgamation is the non-factual procedure used to coordinate, assess and translate the discoveries of different subjective research thinks about. Such reviews might be consolidated to recognize their regular center components and topics. Discoveries from phenomenological, grounded hypothesis or ethnographic reviews might be incorporated and utilized. Not at all like meta-examination, where a definitive aim is to diminish discoveries, meta blend includes dissecting and orchestrating key components in each review, with the point of changing individual discoveries into new conceptualizations and understandings.

4. Discussion

The discussion provided in the literature about industrial espionage shows the continuous alterations of the advantages from corporate crime. The roles of different actors for value creation and capturing the value by stealing technologies can switch dynamically through the centuries (Søilen, 2016). The Global World can face bigger challenges of information security in the future unless the better agreements between governments and businesses are established. Hence, security managers have to be aware of the possible implications of the industrial espionage attacks against their organizations.

Ferdinand and Simm (2007) argue about the limits of the informational input to the organization from illegal sources and give the review of the external learning of the

companies. The threat is identified as a sign of upcoming crisis, “the prodromal stage” Fink (1986, pp. 21-22). In the context of this paper, industrial espionage is a corporate crime and the task for security managers is in evaluating the threats and find the ways of protection from it (I. Winkler, 1997) and (Mendell, 2011).

Finally, Søilen (2016) argues, that early self-taught industrialists voyaging were the standard method for learning. Really, learning by voyaging has been a very much utilized strategy for gaining an upper hand all through history. In this manner, we have completed the cycle with regards to modern undercover work inside a couple of hundreds of years and there is nothing to propose that these exchanging parts of who remain to benefit from spying and who remain to lose will stay static. Rather we may expect that this will keep on changing with the rotations in the upper hand of countries unless a superior arrangement of global laws and assertions can be set up.

5. Conclusion

Above all else, supervisors must recognize that the risk of mechanical undercover work is in a consistent calculation of a contemporary business life. There is no pointer of a decline in movement: it is digging in for the long haul. An inescapable outcome is that all exercises identifying with keeping modern spies from focusing on an association must be nonstop. Also, supervisors must understand their enemies are not straightforward patio analysts, but rather exceedingly gifted proficient spies utilizing a similar reconnaissance strategy whether they work for an administration insight office or a business knowledge equip.

The current methods of the information security mainly focus on the technical aspects of the protection system. Still, with the development of the information technologies, it is impossible to assure full protection from the external attacks of spies. In addition, the concentration of the budget and administrative efforts for security on the technical methods creates the gap in other methods of protection the data from thieves. All the recent scientific articles provide the evidence of the high level of informational outflow with the help of insiders. Hence, the only comprehensive system of preventive methods for espionage threat with all the security disciplines included can maximize the protection of data.

References

[1] Cornwall, H. (1991). *The industrial espionage handbook*: Century.

[2] Cronin, P., Ryan, F., & Coughlan, M. (2008). Undertaking a literature review: a step-by-step approach. *British journal of nursing, 17*(1), 38.

[3] Ferdinand, J., & Simm, D. (2007). Re-theorizing external learning: insights from economic and industrial espionage. *Management Learning, 38*(3), 297-317.

[4] Fink, S. (1986). *Crisis management: Planning for the inevitable*: American Management Association.

[5] Herring, J. P. (1992). Business intelligence in Japan and Sweden: Lessons for the US. *Journal of Business strategy, 13*(2), 44-49.

[6] House, W. (1995). Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. *Washington, DC: Government Printing Office*.

[7] Malone, N., Baluja, K. F., Costanzo, J. M., & Davis, C. J. (2000). The foreign-born population: 2000. *US Census Bureau, US Department of Commerce, Census*, 01-01.

[8] Mendell, R. L. (2011). *The quiet threat: fighting industrial espionage in America*: Charles C Thomas Publisher.

[9] Michalowski, R. J., & Kramer, R. C. (2006). *State-corporate crime: Wrongdoing at the intersection of business and government*: Rutgers University Press.

[10] Nasheri, H. (2005). *Economic espionage and industrial spying*: Cambridge University Press.

[11] Pasternak, G., & Witkin, G. (1996). The Lure of the Steal. *US News & World Report*, 45.

[12] Penenberg, A. L., & Barry, M. (2008). *Spooked: espionage in corporate America*: Basic Books.

[13] Perman, S. (2010). *Spies, Inc.: Business Innovation from Israel's Masters of Espionage*: Pearson Education.

[14] Pitts, J. (2008). *Reluctant gangsters: The changing face of youth crime*: Taylor & Francis.

[15] Polanyi, M. (1967). The Tacit Dimension New York. *Garden City*, 4.

[16] Pontell, H. N., & Geis, G. (2007). *International handbook of white-collar and corporate crime*: Springer.

[17] Rustmann, F. (2002). *CIA, Inc: Espionage and the Craft of Business Intelligence*: Potomac Books, Inc.

[18] Søilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century–Status quaestionis. *Journal of Intelligence Studies in Business, 6*(3).

[19] Thorleuchter, D., & Van den Poel, D. (2013). Protecting research and technology from espionage. *Expert systems with applications, 40*(9), 3432-3440.

[20] Winkler, I. (1997). *Corporate Espionage: what it is, why it is happening in your company, what you must do about it*: Prima Lifestyles.

[21] Winkler, I. S. (1996). *Case study of industrial espionage through social engineering.* Paper presented at the Proceedings of the 19 th Information Systems Security Conference.

[22] Wright, P. C., & Roy, G. (1999). Industrial espionage and competitive intelligence: one you do; one you do not. *Journal of Workplace Learning, 11*(2), 53-59.