Asian Journal of Information Technology 10 (5): 170-179, 2011
ISSN: 1682-3915

Industrial Espionage as a Method of Technology Transfer and How to Prevent it

Hessam Zandhessami, Pouya Majd Pezeshki and Abolfazl Moradian
Department of Industrial Management, Islamic Azad University, Qazvin Branch, Iran

Abstract: The first part of this study summarizes technology transfer methods and then it looks at how espionage has never been easier. This study features a report on who the spies are why they steal electronic data and what techniques they use. Also speculates on what the potential costs of espionage could be to nations and organizations. In order to shed light on the illegal aspects, this study looks at some recent cases of industrial espionage, involving major multinationals. At the other hand we introduced a range of measures that can be taken to reduce the likelihood of becoming a target for industrial espionage and minimize the effects if you are attacked. In this study we study from two perspectives; first from who use industrial espionage techniques to achieve technology and second from who try to protect his own assets contain trade secrets and technologies etc., through necessary prevention measures. So, the researchers introduce industrial espionage techniques which are often used and prevention techniques which should take place. At end we evaluate and rank suitable prevention methods by using group TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) approach. This study implies review industrial espionage cases and finds a quantitative methodology based on a structured framework for ranking the most appropriate prevention method. Send questionnaire to selected managers of information security in high tech organizations in Iran to evaluate each methods of industrial espionage and to find which ones are used more than others and rank the prevention methods to make information secured.

Key words: Industrial espionage, technology transfer, information and communication technology, ethic, group TOPSIS, Iran

INTRODUCTION

Lapse the time and acceleration in technology developments led the companies or countries to not be able to provide all technologies needed. Therefore, it is inevitable to transfer technology from other companies/ countries.

Selection of the appropriate transfer method can be effective in success of process to transfer and absorb the technology transferred to the receiving company/ country and become an indigenous one (Lee, 2002). Technology transfer can be occurred between two or more companies in a country or two or more companies in different countries. Technology transfer is a process in which the technology components transfer from a source to receiver of the current (Radosevic, 1999). Technology transfer is one of the areas created in the field of knowledge, upon which interest of the organizations are growing rapidly (this indicates that these two words are considered as the keys of development and competition) and from which companies use for competitive advantages (Baughn and Osborne, 1989). Technology transfer can be used to increase competitive strength in the whole industry with the boundaries consisting of all countries (Reisman, 1989) which can cause economic improvement and social progress and enhance the quality of life and even culture and values (Reddy and Zhao, 1990).

According to a comprehensive definition, technology transfer is the process of sharing skills, knowledge, technology, production methods, production samples and facilities owned by governments and/or other organizations and institutions which is provided to more users in order to obtain scientific and technological improvement and progress. They use it to improve, develop and create a new method, process, product or service.

Therefore, after assessing the level of technology required to obtain situation, competitive position and after evaluating the existing technology if it is impossible to supply gap and/or if there is no interest to provide at the country level, technology transfer will be used to obtain technology and to fill the existing gape.

Technology transfer process can be generally shown in Fig. 1. As shown in Fig. 1, the transfer process starts from an appropriate transfer method so at first the researchers briefly explain introduce technology transfer methods.

Corresponding Author: Pouya Majd Pezeshki, Department of Industrial Management, Islamic Azad University, Qazvin Branch, Iran

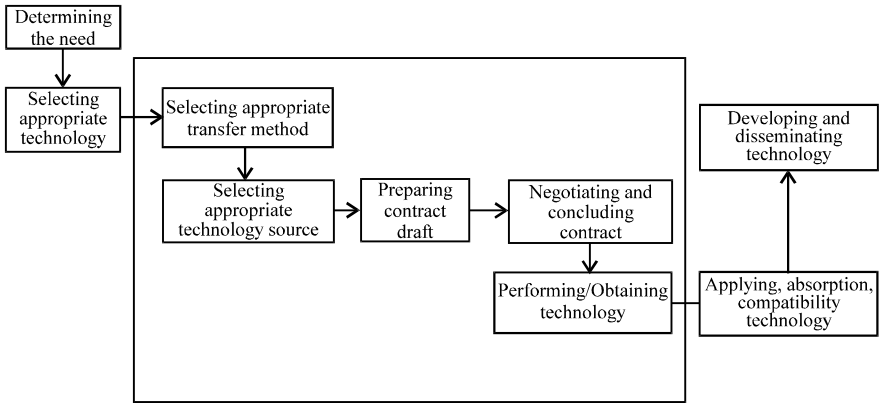

Fig. 1: Technology transfer process (Khalil, 2000; Radosevic, 1999; Sung and Gibson, 2000)

Table 1: Different interpretations about the transfer methods in the literature

Phrases	References
Technology transfer channel	Khalil (2000), Radosevic (1999) Ragaits (1999)
Technology transfer mode	Lee (2002), Radosevic (1999), Kondo (2005), Stainslaw (1996), Cassiman and Veugelers (2000), Chiesa and Manzini (1998)
Technology transfer pathway	Boarini (1999)
Technology transfer mechanism	Khalil (2000), Radosevic (1999), Robert and Berry (1985)

There are different interpretations about the transfer method in the literature which can be briefly shown in Table 1 along with their references then, they are supposed to be the same and are considered as technology transfer methods.

Generally, different methods are mentioned in the literature for transferring technology, some of them are identical in content and nature and only differ in their titles. Here the researchers introduce the most important techniques with combination of some similar techniques.

Obtaining technology through acquisition of a company (Acquisition): In this method, the recipient company buys the technology holder company and owns it instead of transferring technology directly. Obviously, through in this way, the technology will be acquired (Chiesa and Manzini, 1998).

Training acquisition (Human exchange and hiring): In this method, the recipient company, employed experts under certain conditions or uses from other companies professionals services as an agent (Radosevic, 1999; Kondo, 2005; Chiesa and Manzini, 1998).

Merge: In this method, a company merges with another company that is the holder of technology and a new company formed from combination of two previous companies in which technological capabilities are shared. Obviously, in the process of sharing technological capabilities, technology and technical knowledge transferring is happen between the two organizations (Chiesa and Manzini, 1998).

Licensing: In this method, a recipient organization receives all or part of technological rights which is owned by another organization (technology provider) via paying some money or some services. This method to access technology usually is used in food and drug industries and service activities. In this method, technology recipient organization in addition of mastering technology, supply product/service in market using owner's credit and name (Khalil, 2000; Radosevic, 1999).

Joint venture: In this way, two or more firms share their technological power, knowledge and resources to develop a special technology so that a third company which usually has a limited life is created and each part is participating in profit and losses (Khalil, 2000; Robert and Berry, 1985; Chiesa and Manzini, 1998). Usually using joint venture in large projects with high cost and investment risk becomes important (Robert and Berry, 1985).

Alliance: In this way two firms share their technological capabilities in order to achieve new technology (Chiesa and Manzini, 1998) and in spite of many similarities with joint venture method there are some differences which could be mentioned as there is no investment between firms and usually its short term cooperation in alliance (Robert and Berry, 1985).

Training and education: This method is divided to two training and education part:

Education: Employees of recipient company are sent to educate in different grades inside or outside the country under the supervision of technology provider and getting valid scientific documents.

Training: Technology recipient company hold required short and long term practical courses in the provider company or under its auspices. This method has been introduced under other titles such as research and training courses and study abroad (Radosevic, 1999).

Reverse engineering: In this method, the recipient achieves technology through simulation, breaking codes and discover the technology secrets and remaking products (Khalil, 2000). This method has been introduced under other titles such as Imitation and Duplicate copy. This method can be used when access to technology is difficult or impossible and transport costs are high and legal costs are low (Lee, 2002).

Outsourcing: In this method, some activities are transferred outside the company. During this products transition and delivery by contractors which often accompanied by product or manufacturing process control by employer, transfer of technology or technical knowledge is occurred (Kondo, 2005).

Turn key project: In this method receiver, purchase technology in the form of a complete project from technology holder so that technology provider manages and run the design, installation and initial operation process. In certain cases, training and support after launching is also part of the agreement (Khalil, 2000).

Equity investment: Investment in other companies result in access to technology and has several forms. It is possible that recipient company invests in the source company to access their technical knowledge or the source company invests in recipient so the technology transferred (Lee, 2002). This investment could be as equal or minority shares. In the minority share method, one company buy part of the supplier company's share but it has no role in its management (Chiesa and Manzini, 1998).

R and D collaboration: Cooperation in research and development is possible in different ways:

Joint R and D: Two companies decide to search jointly in R and D areas about a particular technology without having to buy each other's share (Chiesa and Manzini, 1998).

R and D contract: A company undertakes costs of research projects in academic or research centers to develop a specific technology (Chiesa and Manzini, 1998).

Contract out R and D: In this method, the organization defines part of his R and D activities as a project and assign to other organizations as a contractor agreement (Khalil, 2000).

Industrial espionage: Is a technique to gain technical information and transferring the technology without permission from the owner of information or technology. Although, there are ethical doubts about this method due to illegal actions which are known as a crime but sometimes it may become a logical decision to achieve required information and technology (Lee, 2002).

Industrial espionage is a technique to gain technical information and transferring the technology without permission from the owner of information or technology. Although, there are ethical doubts about this method due to illegal actions which are known as a crime but sometimes it may become a logical decision to achieve required information and technology.

This method is often used in high-technology industries which leads technology and market to be progressive. Industrial espionage is sometimes done by companies and their experts and sometimes by the information brokers whose role in technology transfer has been shown in Fig. 2.

Information broker: The value of information in business creates the opportunity to make money both legally and illegally. Information broker is a middle man who will obtain information from one source and sell it to organizations that want it. At one end of the spectrum this is a perfectly legitimate and well-established and respected business that has its own trade representation in organizations such as the Society of Competitive Information Professionals but at the other end it can be criminal. Now we have countries spying on behalf of their national industries as well as for military and political secrets, companies trying to steal other companies' sensitive information and independent brokers who will

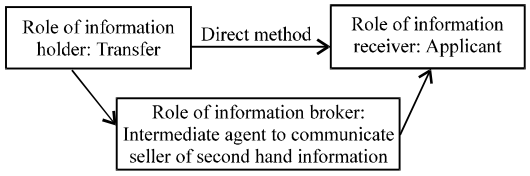

Fig. 2: Information broker roles

buy information from anyone if they think that there is a market for it. We all have the own preconceptions of the type of people that will be involved in industrial espionage but as with some of the successful practitioners in other areas, the good ones do not necessarily fit the profiles. After all, all of the best spies for governments were well placed and trusted by their employers as you wouldn't be much of a spy if you were not.

Selecting appropriate technology transfer method has a great impact on the success of the transfer process. It should be noted that a complete technology transfer sometimes requires the use of a combination of several different methods (Ragaits, 1999).

Necessity of research from the perspective of information receiver: This approach needs less cost for the information obtaining companies. Furthermore, the resources lost by the goal organization will be regarded as revenue of the receiving organization. High research and development costs paid by the leading organizations will be easily provided for rival company through industrial espionage.

Necessity of research from the perspective of information watcher: It is unfortunately, a reality that in the majority of cases, the security of information is reactive, it responds to each of the new methods that are used to attack it once the attacks become known. Put another way, it is normally only after a successful attack has been detected that new measures are put in place to prevent a recurrence. The down side of this is that an attack may be successful and remain undetected for a considerable period.

Data: In today's hi-tech world, the intelligence requirements of a number of countries also include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields. In other words, the targets have moved from being just government departments to include research and industry. The researchers will look at how espionage has never been easier. It seems reasonable to start with the question What is industrial espionage? This may seem a stupidly simple question which has an obvious answer companies spy on other companies! Unfortunately, to presume that would be a gross over-simplification. Espionage as most people understand it is one country spying on another country to obtain political or military advantage. Industrial espionage also known as corporate or business espionage is spying that is conducted for commercial rather than national security purposes. However, it may be carried out by governments, companies and by other types of private organizations such as pressure groups. In the most straightforward cases, it is corporations spying on competitors to gain a market advantage which probably entails the theft (or copying) of trade secrets and/or confidential or valuable information for use. In less commonly reported or understood scenarios, it may be a government spying on a corporation to gain information that will be of benefit to its own national military, industrial or commercial base. The types of material that are most often targeted are companies research and development, designs, formulas, manufacturing processes and future plans.

Despite such a situation and in continuing the research done, this question has been considered as the subject of this research: How information-obtaining methods can be identified through industrial espionage and how organization knowledge and information can be protected against the spies?

Some cases of industrial espionage: There have been a number of well documented cases where company to company industrial espionage has been alleged:

- In formula 1 motor racing between Ferrari and McLaren (Solitander and Solitander, 2010)
- Again, in the US, it was reported that Wal-Mart regularly sent its department managers into Kmart, one of its main competitors to electronically scan equivalent products and the prices at which they were being offered (Jones, 2008)
- Another incident of industrial espionage involved the companies Procter and Gamble and Unilever. In 2001 when it came to light that private investigators hired by Procter and Gamble in the United States, to find out more about its competitor's hair care business had sifted through rubbish bins outside Unilever's offices. The investigators succeeded in gathering piles of unshreded documents relating to Unilever's plans for the shampoo market (Crane, 2005)
- Other cases of industrial espionage that have made the news include the well publicized 2006 reports of three people who were convicted in the US of plotting to steal trade secrets from the soft drink maker Coca Cola and trying to sell them to its main competitor, Pepsi (Macleod, 2006)
- Other examples include the dispute between Volkswagen AG (VW) and General Motors (GM) which accused a former GM purchasing chief, of stealing its trade secrets when he left GM in 1993 to move to VW (Litkowski, 2005; Effron, 2004)
- The Veterans Affairs Department agreed to pay a total of $20 million to veterans for exposing them to possible identity theft in 2006 by losing their personal information. The case began after a laptop computer was stolen in a burglary at the Maryland home of a department data analyst. The laptop and

an external drive contained data that the analyst had taken home without permission including the names, birth dates and Social Security numbers of up to 26.5 million veterans and active-duty service members

There are many cases of espionage by a nation state against both governments and companies in order to obtain political or military advantage for example it could be mentioned:

- An example of espionage by a nation state against both governments and companies is a range of attacks originating from China called Titan Rain. The attacks which started in 2005 show the massive scale that such activity can take. The case involved Chinese hackers, some believed to be from the People's Liberation Army (PLA), attacking the computer networks of US military and government sites, British government departments and also those of Germany (Jones, 2008)
- The 2 years later in 2007, the American Intelligence website reported that China had allegedly tried to hack into highly classified government computer networks in Australia and New Zealand. The report stated that this was part of a broader international operation by the Chinese to glean (Jones, 2008)
- Another country that is one of the most aggressive collectors of economic intelligence in the world is France. The researchers accuses the French government of infiltrating numerous American companies including IBM, Texas Instruments and Corning which among other things, produce cutting edge fibre-optics, semiconductors and advanced materials for the telecommunications industry. They established of the Cole de Guerre Economique (EGE) (School of Economic Warfare) as an example of the French attitude to the issue (Nolan, 1999)

MATERIALS AND METHODS

Identifying industrial espionage methods: So what techniques are being used today for industrial espionage? The advent of the computer and its use by all types of organizations has revolutionized industrial espionage. In the past the techniques ranged from breaking and entering an establishment and stealing or photographing significant documents to planting a person to work in the organization and paying an existing employee to betray the organization and a whole host of other techniques. Since, the computerization of a vast range of aspects of business and personal life, the way in which these techniques are used has changed and many new techniques have been developed to take advantage of the new environment. The volumes and types of information that are now stored electronically means that protecting data has become more difficult. It is unfortunately, a reality that in the majority of cases, the security of information is reactive, it responds to each of the new methods that are used to attack it once the attacks become known. Put another way, it is normally only after a successful attack has been detected that new measures are put in place to prevent a recurrence. The down side of this is that an attack may be successful and remain undetected for a considerable period (Fig. 3). Here, the researchers introduce some espionage methods.

Laptop theft: One of the techniques that take advantage of the new technologies that are currently being used is the theft of laptops and other computers.

Spyware: Another technique that is being used extensively at the moment is that of the planting of spyware. Spyware is software that is installed surreptitiously on the target computer usually to monitor the user's behavior or collect an array of information and store or transmit it to a designated site.

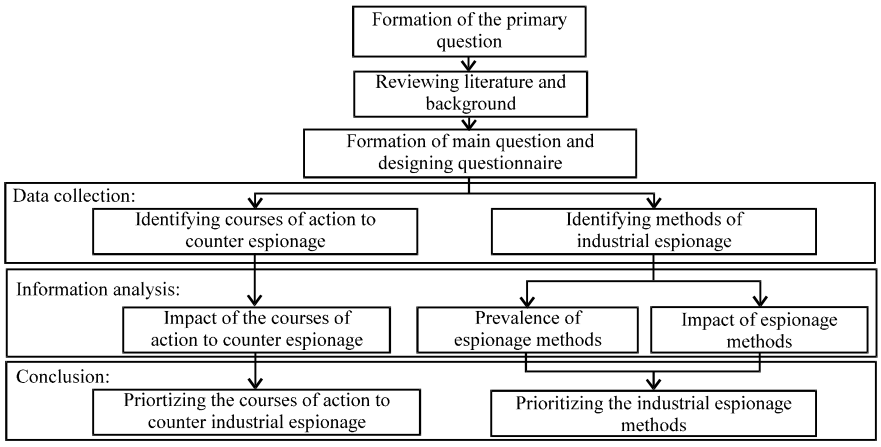

Fig. 3: Stages of research

Key loggrer: A key loggrer does just what its name implies, it logs the keystrokes of the user and is normally used to capture information such as user names and passwords.

Back doors: The technique favored by many people attempting to gain access to computer systems at the moment is the planting of software that creates a back door on the computer that allows it to be controlled by the miscreant. Once they have control of the computer, they can copy the information they want, monitor what is going on and use the computer for their own ends, perhaps even using it to spy on the target company's competitors and get it blamed.

Steganography: If the person has access to the computer (one of your trusted staff), a technique that can be used to get information out is the hiding of information in other, apparently innocent files. This is known as Steganography (secret writing) and gives the miscreant the opportunity to send files that appear to be totally innocent-perhaps a music clip or a picture that also contains large quantities of sensitive information. Although, there are no detected cases of Steganography happening in industrial espionage, it is probably only a matter of time.

Surveillance: Then there are techniques such as wire and fibre tapping and wireless signal interception where the signal being transmitted is intercepted en-route. Alternatively, there is also the good old-fashioned technique of surveillance using modern technology such as directional microphones, laser microphones, telephone tapping and the bugging of rooms.

Stealthy copy and move: Modern mobile phones have a significant data storage capability, together with high resolution cameras and can communicate using infrared, bluetooth and Wi-Fi in addition to the expected GSM connection. The laptop that in many cases is the only computer an employee will use, now also has all or most, of that functionality. USB storage devices, micro drives and flash memory cards have replaced the humble floppy disk and in addition to being much smaller and easier to hide also have significantly greater storage capacities.

Identifying courses of action to confront industrial espionage: In the past, people tended to work for an organization with the intention of a full career with it and as a result, there was a higher degree of loyalty and also of self-interest. After all if the company was disadvantaged or went out of business that person's job was likely to go as well. In recent times, there has been a move to a more mobile work force with career development and salary advancement being gained by moving to a new company and position every 3 years or so. With this comes the reduction in loyalty and ownership and also of course, some of the corporate knowledge will inevitably also move with the individual. All of these changes contribute to an increasingly difficult environment in which information that is of value and importance to an organization must be protected. In reality, what can be done is to put into place the appropriate security measures across all aspects of the environment. This must be an integrated approach that covers the physical security of the establishments, the personal security of staff, the procedural measures that are put in place and the electronic security measures that are additional to all of the other types of measures.

Unfortunately, in information security, the most widely accepted convention has been that we need to keep the bad people out of the systems and we have relied heavily on perimeter defenses, often to the detriment of internal measures.

There are a range of measures that can be taken to reduce the likelihood of becoming a target for industrial espionage and minimize the effects if you are attacked: making sure that information security risk assessments have been carried out. All of the normal physical, personnel and procedural and electronic security measures have been implemented. Cryptography has been available for a number of years and while the cost of using it was initially significant, the cost of acquisition and management is now at a more realistic level. For highly sensitive material, it could be stored in such a way that no one individual had access to it by measures such as the two man rule where two separate locks had to be released and the keys were held by two different, trusted individuals. The individuals who had access to the material were checked and their credentials verified. They could be monitored and if they attempted to remove documents or materials, they were likely to be detected by physical checks at access points. When information systems were first introduced, the security systems were modified to cater for the new technology and the means of copying or removing information were tightly controlled. Particular attention should be paid to laptop computers and any material that is likely to leave the secure confines of the organization. Another gap occurred when the type of technology that in the past was considered to be of too high a risk was introduced. For example, items such as laptop computers and mobile phones became so integrated into the normal business

process that it was no longer feasible to prevent their use in areas where sensitive information was in use. Most organizations would find it a significant impediment to exclude them these days. Once the first generation of these devices was accepted, the gap widened at a rapid rate as the functionality of these devices increased. Modern mobile phones have a significant data storage capability, together with high resolution cameras and can communicate using infrared, bluetooth and Wi-Fi in addition to the expected GSM connection. The laptop that in many cases is the only computer an employee will use, now also has all or most of that functionality. USB storage devices, micro drives and flash memory cards have replaced the humble floppy disk and in addition to being much smaller and easier to hide also have significantly greater storage capacities. The system administration staff regularly had unrestricted access to it after all, they were the people who were responsible for managing the operation of the systems and the storage of information and helping the user to gain the maximum benefit from it. The gap here occurred because the computer systems staff was considered to be technicians and the control of their access to sensitive information is not always recognized or properly controlled. In addition, all the other members of staff who did not have a need to know the material would probably have been using the same network which created the potential for them to gain access to the sensitive information, either by accident or omission of the security measures or by malicious intent. To ensure that the organizations' internal networks are not visible to people outside. For this purpose it is highly recommended to use Firewalls, Anti-Hack and Anti-Spy software. Sensitive information should be stored in a secure manner and only held for as long as it is required. It makes sense wherever it is possible, to store it in an encrypted form whether it is on the computer or on the offline storage media. In order to protect against the potential loss of sensitive information, a suitable regime of backups and offsite storage should be arranged. With a suitable access control and auditing system, the ability to identify attempts to access information to which staff are not authorized or to tamper with sensitive data should be deterred or detected.

Statistical population and data collection tools: In this study, the population includes those senior managers of single industries of the country whose organization is likely to be encountered with espionage attacks, especially on the information technology and those selected as experts in this field.

To collect data, two questionnaires with the following titles were developed and given them:

- Questionnaire on studying amount of familiarity with espionage methods and determining the effectiveness of each method to obtain knowledge
- Questionnaire on studying interaction of the coping and prevention methods and espionage methods

After completing the questionnaire, the results were analyzed as the statistical data whose results are given in the next sections.

Technique: TOPSIS (Technique for Order Performance by Similarity to Ideal Solution) is a useful technique in dealing with Multi Attribute or Multi-criteria Decision Making (MADM/MCDM) problems in the real world (Hwang and Yoon, 1981). It helps Decision Maker (s) (DMs) organize the problems to be solved and carry out analysis, comparisons and rankings of the alternatives. Accordingly, the selection of a suitable alternative (s) will be made. However, many decision making problems within organizations will be a collaborative effort. An extension of TOPSIS for group decision making (Shih *et al*., 2007): to include the multiple preferences of >1 DM, the researchers will consider the separation measures by taking the geometric mean or arithmetic mean of the individuals for TOPSIS. The detailed procedure with a few options within each step is illustrated in the following.

Step 1: Construct decision matrix D^k, k = 1, ..., K for each DM. The structure of the matrix can be expressed as follows:

$$D^k = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccccccc} X_1 & X_2 & \cdots & X_j & \cdots & X_n \end{array} \\ \begin{bmatrix} x_{11}^k & x_{12}^k & \cdots & x_{1j}^k & \cdots & x_{1n}^k \\ x_{21}^k & x_{22}^k & \cdots & x_{2j}^k & \cdots & x_{2n}^k \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ x_{i1}^k & x_{i2}^k & \cdots & x_{ij}^k & \cdots & x_{in}^k \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ x_{m1}^k & x_{m2}^k & \cdots & x_{mj}^k & \cdots & x_{mn}^k \end{bmatrix} \end{array} \quad (1)$$

where, A_i denotes the alternative (technology transfer methods) i, i = 1, ..., m$_i$X$_j$ represents the attribute or criterion j, j = 1, ..., n with quantitative and qualitative data. x_{ij}^k indicates the performance rating of alternative A_i with respect to attribute X_j by decision maker k, k = 1, ..., k and x_{ij}^k is the element of D^k. It is noted that there should be K decision matrices for the K members of the group.

Step 2: Construct the normalized decision matrix R^k = k = 1, ... K for each DM. For DM k, the normalized value r_{ij}^k of the decision matrix R^k can be any linear-scale transformation to keep $0 \le r_{ij}^k \le 1$ as follows:

$$r_{ij}^{k}=\frac{x_{ij}^{k}}{\sqrt{\sum_{j=1}^{n}\left(x_{ij}^{k}\right)^{2}}} \quad (2)$$

Where, i = 1, ..., m; j = 1, ..., n and k = 1, ..., k.

Step 3: Determine the ideal and negative ideal solutions V^{k+} (PIS) and V^{k-} (NIS), respectively for each DM k = 1, ..., K. For DM_k, his or her PIS and NIS are:

$$\begin{aligned} V^{k+}&=\left\{r_1^{k+},...r_n^{k+}\right\}=\left\{\left(\max_i r_{ij}^{k}\,|\,j\in J\right),\left(\min_i r_{ij}^{k}\,|\,j\in J'\right)\right\}\\ V^{k-}&=\left\{r_1^{k-},...r_n^{k-}\right\}=\left\{\left(\min_i r_{ij}^{k}\,|\,j\in J\right),\left(\max_i r_{ij}^{k}\,|\,j\in J'\right)\right\}\end{aligned} \quad (3)$$

Where:

J = Associated with the benefit criteria

J' = Associated with the cost criteria; i = 1, ..., m; j = 1, ..., n and k = 1, ..., K

Step 4: Assign a weight vector W to the attribute set for the group. Each DM will elicit weights for attributes as w_j^k where, j = 1, ..., n and:

$$\sum_{j=1}^{n} w_j^{k}=1$$

and for each DM k = 1, ..., K. Each element of the weight vector W will be the operation of the corresponding elements of the attributes weights per DM.

Step 5: Calculate the separation measure from the ideal and the negative ideal solutions, $\overline{s_i^{+}}$ and $\overline{s_i^{-}}$, respectively for the group.

There are two sub-steps to be considered in step 5. The first one concerns the distance measure for individuals; the second one aggregating the measures for the group.

Step 5a: Calculate the measures from PIS and NIS individually as follows:

$$S_i^{k+}=\sqrt{\sum_{j=1}^{n} w_j^{k}\left(v_{ij}^{k}-v_j^{k+}\right)^{2}},\ \text{for alternative i, i=1,...,m} \quad (4)$$

And:

$$S_i^{k-}=\sqrt{\sum_{j=1}^{n} w_j^{k}\left(v_{ij}^{k}-v_j^{k-}\right)^{2}},\ \text{for alternative i, i=1,...,m} \quad (5)$$

Step 5b: Calculate the measures of PIS and NIS for the group. In addition, the group separation measure of each alternative will be combined through an operation ⊗ for all DMs, k = 1, ..., K. Thus, the two group measures of the PIS and NIS are the following two equations:

$$\overline{S_i^{+}}=S_i^{1+}\otimes...\otimes S_i^{K+},\ \text{for alternative i} \quad (6)$$

$$\overline{S_i^{-}}=S_i^{1+}\otimes...\otimes S_i^{K+},\ \text{for alternative i,} \quad (7)$$

The operation can offer many choices, geometric mean, arithmetic mean or their modification. If we take the geometric mean of all individual measures, the group measures, Eq. 4 and 5, from PIS and NIS will be:

$$\overline{S_i^{+}}=\left(\prod_{k=1}^{K} S_i^{k+}\right)^{\frac{1}{K}},\ \text{for alternative i,} \quad (8)$$

And:

$$\overline{S_i^{-}}=\left(\prod_{k=1}^{K} S_i^{k-}\right)^{\frac{1}{K}},\ \text{for alternative i} \quad (9)$$

where, i = 1, ..., m; k = 1, ..., K. Results of step 5b are shown in Table 2.

Step 6: Calculate the relative closeness to the ideal solution for the group. Calculate the relative closeness $\overline{C_i^{*}}$ to the ideal solution and rank the alternatives in descending order. The relative closeness of the ith alternative A_i with respect to PIS can be expressed as:

$$\overline{C_i^{*}}=\frac{\overline{S_i^{-}}}{\overline{S_i^{+}}+\overline{S_i^{-}}},\ i=1,...,m \quad (10)$$

Where, $0\le \overline{C_i^{*}} \le 1$. The larger the index value, the better the performance of the alternative.

Step 7 (Rank the preference order): A set of alternatives can now be preference ranked according to the descending order of the value of $\overline{C_i^{*}}$. Results of step 6 and 7 are shown in Table 3.

Table 2: The separation measure of alternatives for the group

	Separation measure of the group	
No.	$\overline{S_i^{+}}$	$\overline{S_i^{-}}$
1	0.066625	0.080357
2	0.048799	0.111454
3	0.090531	0.068830
4	0.107008	0.060251
5	0.073564	0.072299
6	0.072533	0.088348
7	0.081521	0.087269
8	0.124392	0.052454
9	0.069123	0.073125
10	0.089867	0.073971
11	0.109765	0.051544
12	0.060915	0.077696

The separation measure of the group is counted through the geometric mean of all DMs with Euclidean distance and vector normalization

Table 3: The relative closeness and rank by group TOPSIS

No.	$\overline{C_i^*}$	Courses of action to confront industrial espionage	Rank	Note
1	0.546712	Making sure that information security risk assessments have been carried out	4	
2	0.695487	Normal physical, personnel and procedural and electronic security measures have been implemented	1	*
3	0.431914	Cryptography	9	
4	0.360225	Two-Man Rule	10	
5	0.495662	The security systems were modified when information systems were first introduced	7	
6	0.549152	Attention to laptop computers and any other instrument such as mobile phone, bluetooth, Wi-Fi, GSM, USB storage devices, micro drives and flash memory cards	3	
7	0.517027	Control the access of system administrator staff	5	
8	0.296607	To ensure that the organizations' internal networks are not visible to people outside	12	#
9	0.514066	Sensitive information should be stored in a secure manner and only held for as long as it is required	6	
10	0.451488	To store information in an encrypted form whether it is on the computer or on the offline storage media	8	
11	0.319535	Provide backups and keep information in off-site storages	11	
12	0.560534	To control the access and auditing system, the ability to identify authorization to access information for each staff	2	

* and # marks the first and the last candidate, respectively

Data collection: To collect data, the questionnaires were distributed between eleven experts on IT and information protector in different organizations by which amount of familiarity with the espionage, effectiveness of the technology transfer methods and courses of action to counter industrial espionage and amount of effectiveness of the coping methods to prevent any espionage method were questioned.

The results per person were received as matrix form and after conversion of qualitative into quantitative variables of the results for each expert was done, calculation of the relative closeness $\overline{C_i^*}$ to the ideal solution for the group by using the geometric mean is shown in the Table 3.

CONCLUSION

While information of the organizations is very high in size, it is being stored in networks which are also at risk of attack. There are many measures to protect sensitive information which haven't been done in most organizations the following can be cited as the main reasons:

- Difficulty and problems related to implementation of protection systems
- Lack of proper understanding of the costs, due to stolen information, imposed to the organization

If organizations want to remain in the competition arena, they should consider very strong precautions to protect their information. Although, observation of the samples from the organizations faced with espionage attacks may cause smile, the researchers are always concerned that these events to be occurred in the organization. The fact is that to improve their activities, the organizations have to use technology which makes very easy to implement the industrial espionage.

Considering the results of questionnaires about the industrial espionage methods in Iran, personal computers, memory disks, mobile phones, USB memory, hard drive and bluetooth, Wi-Fi, GSM and very small memory cards have the most use and effectiveness for data transfer and industrial espionage and it seems that to counter industrial espionage, the most effective method is to evaluate the physical tools, personnel and processes to perform tasks as well as to control access to information through identifying options and levels of the individuals access to information and to control tools of copying and handling information (such as memory cards, mobile phone and so on).

LIMITATIONS

Considering the following cases, it is impossible to study and analyze the effectiveness of each coping method as pre-occurrence and only the comments by experts are sufficed:

- In most cases, after the espionage attacks, the companies take notice or sometimes they will not even notice
- On the other hand, each time after the attack, the software used to counter espionage are updates and are ready to counter the next attack of the same type
- There is always the possibility to penetrate the spies with completely new methods in the information division of the organizations

RECOMMENDATIONS

It is recommended on industrial espionage that the company attacked by spies be evaluated as a case and the coping courses of action and ones to strengthen them for future cases be proposed.

REFERENCES

Baughn, C.C. and R.N. Osborne, 1989. Strategies for successful technological development. J. Technol. Transfer, 14: 5-13.

Boarini, E., 1999. Inbound Technology Transfer. In: Technology Management, Szakonyi, R. (Ed.). Auerbach, New York, pp: 1-11.

Cassiman, B. and R. Veugelers, 2000. External technology sources: Embodied or disembodied technology acquisition. Department of Economics and Business, Universitat Pompeu Fabra, Economics Working Papers No. 444. http://ideas.repec.org/p/upf/upfgen/444.html.

Chiesa, V. and R. Manzini, 1998. Organizing for technological collaborations: A managerial perspective. R&D Manage., 28: 199-201.

Crane, A., 2005. In the company of spies: When competitive intelligence gathering becomes industrial espionage. Bus. Horizons, 48: 233-240.

Effron, R.J., 2004. Secrets and spies: Extraterritorial application of the economic espionage act and the trips agreement. Barnard College, Columbia University; J.D. Candidate New York University School of Law.

Hwang, C.L. and K. Yoon, 1981. Multiple Attribute Decision Making and Applications. Springer-Verlag, New York.

Jones, A., 2008. Industrial Espionage in a Hi-tech world. Comput. Fraud Secur., 2008: 7-13.

Khalil, M.T., 2000. Management of Technology. McGraw Hill, Boston, USA.

Kondo, M., 2005. Networking for technology acquisition and transfer. Int. J. Technol. Manage., 32: 154-175.

Lee, G.A., 2002. Negotiating technology acquisition: Getting the tools you need to succeed. Working Paper, Nanyang Technology University.

Litkowski, K.C., 2005. Evolving XML summarization strategies in DUC. CL Research, 9208 Gue Road, Damascus, MD 20872. http://duc.nist.gov/pubs/2005papers/clresearch.pdf.

Macleod, C., 2006. Industrial espionage: Protect and survive. European Director of Cyber-Ark. September 21, 2006.

Nolan, J.A., 1999. A case study in French espionage: Renaissance software. Chairman and Managing Director of Phoenix Consulting Group. http://www.hanford.gov/oci/maindocs/ci_r_docs/frenchesp.pdf.

Radosevic, S., 1999. International Technology Transfer and Catch up in Economic Development. Edward Elgar Publishing Limited, Massachusetts, USA.

Ragaits, R., 1999. Early Stage Technologies: Valuation and Pricing. John Wieley and Sons, Newe York.

Reddy, M. and L. Zhao, 1990. International technology transfer: A review. Res. Policy, 19: 285-307.

Reisman, A., 1989. Technology transfer: A taxonomic view. J. Technol. Transfer, 14: 31-36.

Robert, E. and C. Berry, 1985. Entering New Business: Selecting Strategies for Success. Cambridge, Mass, Massachusetts Institute of Technology, Boston, USA.

Shih, H.S., H.J. Shyur and E.S. Lee, 2007. An extension of TOPSIS for group decision making. Mathem. Comput. Modell., 45: 801-813.

Solitander, M. and N. Solitander, 2010. The sharing, protection and thievery of intellectual assets: The case of formula 1 industry. Manage. Decis., 48: 37-57.

Stainslaw, K., 1996. Technology transfer and the restructuring of new market economics: The case of Poland. Steep Discussion, Paper No. 32. http://www.sussex.ac.uk/Units/spru/publications/imprint/steepdps/32/steep32.pdf.

Sung, T.K. and D.V. Gibson, 2000. Knowledge and technology transfer: Levels and key factors. University of Texas. http://in3.dem.ist.utl.pt/downloads/cur2000/papers/S04P04.PDF.