International Journal of Social Sciences and Humanities Research

ISSN 2348-2990

Volume 4, Issue 2, February 2016, pp. 1-10

homepages: http://ijsshrjournal.com/

Economic Espionage and Security in Financial Information Systems

Ruhollah Tavallaee(Ph.D)[1], Hossein Rajabdorri[2*]

[1] Assistant Professor in, Shahid Beheshti University, Tehran, Iran
[2] Masters Student in Accounting, Hafez Higher Education Institute, Shiraz, Iran

*Corresponding author's E-mail: Hosrado@gmail.com

ABSTRACT

Nowadays, as trade and commerce becomes more complex at every level, the factors affecting business and trade such as economic information have become increasingly important. Economic information has become a criterion for an organization's superiority over its competitors. Economic information is the commercial organizations' key to success; it includes classified information such as the news and knowledge about research and development, production capacity, financial resources, target markets, and etc. The organization which holds such information is considered to have the winning hand in the competition. If such classified information is leaked, the organization will sustain damage and loss. Economic stability and sustainability and improvement of competitive advantage in business markets are not possible without possession and protection of vast financial information. In the meantime, the information faces threats. It may be willingly or unknowingly leaked by individuals who have access to it, or it might be sought and stolen by competitor organizations which would benefit from the organizations loss. For that matter, guarding and protection of such information is a vital issue. The present article studies the ways to prevent information leak and economic espionage with the purpose of enhancing the accuracy and vigilance among managers.

Keywords: security, information system, economic espionage, accounting.

1. Introduction

Accounting is considered to be the heart of an organization without which organizational activities would have no meaning. By providing economical information, financial reports, and primary requisites of decision-making, accounting facilitates decision-making, hence, playing an important and undeniable role in an organization. If we accept that economic power is an advantage in today's competitive business environment and that organizations with better financial and economic conditions wield greater power, then we have automatically confirmed the important role of decision-making in organizations. That is because success is the result of correct decision-making, and correct decisions are the results of access to effective and up-to-date information. Information is the most valuable commodity in today's world and should be considered as the fundamental asset of any organization. Analogous to electricity without which many businesses can not easily work, information is the most important asset of an organization and is the most vital factor in organizational success (Niekerk & Solms, 2010). In this sense, the highest level of management which is responsible for organizational success is also responsible for protection of organizational information (Ozkan & Karabacak, 2010). Development of information systems is like a double-edged sword; on one hand it brings forth countless benefits for humanity, and on the other hand it causes irreversible damages due to the issue of information security (Yuan & Chen, 2012). For that purpose and in order to prevent information leak, the security of the information must be controlled by the managers. The purpose of information security management in any organization is to protect organizational assets (software, hardware, information and communication, and human resources) against all threats (unauthorized access to information, threats posed by the environment, and risks created by the users). In order to realize this goal a consistent plan is required (Moosavi et al, 2015). Information security management is a subset of information management that provides solutions alongside determining objectives of security and analyzing the obstacle before that. Security management is also tasked with implementation and control of organizational security system and tries to keep the system up-to-date at all times. There are vast studies on information security. These studies include technical, behavioral, managerial, philosophical, and organizational methods which deal with risk reduction and protection of informational assets in computer-based systems (Crossler, 2013). Considering the constructive role of information, protection of information against threats, rubbery, and espionage is a vital issue which helps to use the obtained information to proceed toward organizational objectives in the best possible way.

2. Literature Review

Accounting information system and its importance in the organization

A system is a set of elements with interactive relationships brought together for a common and definite purpose. Another characteristic of a system is the presence of order in the relationship between the elements, in a sense that each element has a predetermined role (Sajadi & Tabatabai

Nejad, 2006). In other words, a system is an ordered set of inter-connected elements which interact with each other to achieve a common goal (Vadiei & Mohammadi, 2010).

Any organization with any kind of performance and activity needs a management information system designed in correspondence to its needs and structure for the purpose of data analysis and decision-making. Accounting information system is an important part of management information system. Considering the importance of financial resource management, accounting information systems are deemed highly important. Implementation of a suitable information system in an organization facilitates the achievement of optimal conditions. Generally speaking, accounting information system helps management in decision-making in order to maintain the organization's strategic position (RajabDorri, 2014). Nowadays, designing accounting information systems has become a specialized branch of accounting. For the purpose of strategic decision-making, managers need the information which is usually provided by accounting information systems (Pourheidari, 2006).

Accounting information system offers the managers the highest extent of information needed to carry out their tasks. The use of correct, accurate, and timely information in the process of decision-making, planning, and other managerial affairs can highly affect organization's performance and efficiency. Knowledge of the correspondence between accounting information systems' capabilities and organization's informational needs lead to identification of weaknesses and strengths in the system (Ghodsi & Salimi, 2013). Accounting information systems are considered to be the most vital and fundamental systems in an organization because they focus on identification and understanding of tasks of accounting systems including collection of the data related to organizational activities and financial phenomena, methods of interpretation of the data into information which can be used by the management, and methods to confirm information accessibility and reliability (Davis, 1997). The main task of information systems is to process the data. However, sometimes it is assumed that organization information systems only deal with the simple processing of raw and primary data on financial and non-financial phenomena affecting organizational activities. Yet the truth is that different levels of management deal with various problems which are different in terms of complexity, and the systems which can help solve this variety of problems are on a spectrum ranging from retrospective information systems to intelligent prospective systems; securing these systems is an important issue which must be taken seriously (Arabmazar Yazdi, 2006).

The importance of information security in accounting information system

Considering the discussed issues about the importance of accounting information system and its determining role, retention and protection of information seems crucial. The term "information security" is defined as the protection of information and information systems against unauthorized access and usage (Safaei, 2004). Controlling information systems especially when they are not properly secured is essential because there are numerous issues posing a threat on these systems (Ariya, 2001). Lack of information security is the cause of major concern for business units and non-commercial organizations. For that reason, accountants and managers should be completely familiar with all types of threats and security issues in order to protect the

programs and information they use (Daily, Lueblfing, 2000). In this system, factors such as information protection and classification are extremely important. Considering the importance of accounting information system and its defining role in decision-making, if the information is not retained and protected in today's competitive environment, the management can not keep competing with other organizations. It must be noted that managers should never neglect the issue of security in information systems because if the information is leaked, the organization will sustain serious damages and losses. To confront this issue, methods of information protection to prevent information leakage such as information zoning and classification, encryption, identification of ways to infiltrate information systems and fixing the weak links, determining the personnel who are authorized to access classified information, detection of unauthorized entry, use of smart cards, and training the personnel on speech protection can be used. It is necessary to mentioned that organizations are not only faced with internal threats and possibility of information leak by internal staff and employees; other factors such as economic and corporate espionage are also external factors posing a threat. These external factors are discussed later in the present paper.

Economic information espionage and its purposes

Based on the definition of the Canadian intelligence service, economic information is the economic or commercial policies including technological, financial, and commercial data or governmental information which if accessed directly or indirectly by foreign actors it would give them relative advantage in economic competition (Nasheri, 2005). There is no doubt that accurate economic information helps with better allocation of organizational resources and provides competitive advantage. If we consider resource limitation and the importance of budget management alongside the issue of competition and innovation, the concept of economic espionage becomes relatively significant. Although economic espionage is not a new concept, the use of new methods and complexity of business in the markets have brought this issue to attention once more. Economic espionage is the attempts made by governments to steal economic information from each other (Nasheri, 2005). According to James Woolsey the former director of US central intelligence agency (CIA), economic espionage is currently the hot issue of information policies (Gadson, Roy et al. 2001; Porteous, 1994). In general, espionage means looking for secrets in order to disclose them; and spying on secrets of economy and trade is a special part of espionage which focuses on secrets and information of commercial and economic nature (Ghaemi et al, 2012). Organizations that do not have enough research and development budget and fall behind their competitors and have doubts about long-term economic growth are more prone to attempt on economic espionage. That is because they do not want to fall behind their competitors, so they use spying methods to compensate for the existing shortcomings in order to ensure their survival in the competition. Off course it must be noted that these assumptions all neglect the professional work ethics. If the ethics are held high in professional communities, then no organization would attempt on such an immoral act which is a kind of robbery.

The concept of economic espionage has also been mentioned in criminal law. There used to be no definition of economic espionage in Iran's criminal law before legislation of the act of electronic trade (Rahbari, 2009). After this law was passed in 2003, the article 65 dealt with business secrets for the first time. According to this article, the commercial secrets are defined as: "the communication data includes all information, formulas, models, software programs, instruments and methods, techniques and processes, unpublished articles, business methods, techniques, plans and procedures, financial information, customer lists, business plans, and alike which have independent economic value and undisclosed to the public and are being protected via reasonable attempts".

The law defines conditions for economic information, that is, the information must be economically valuable, and the classified information can be directly exchanged with money. This means that the holder of business secrets has a competitive advantage over those without that information, otherwise, these information are not legally protected as business secrets (Rahbari, 2009). The other condition is that the secrets mentioned in this article must not be deemed as general information; as soon as the information is disclosed to the public it will loses its legal protected status (Botler, 2001). The third condition is that in order to keep the mentioned information secret, proper reasonable measures should be taken (Post, 2005).

Also, a look at the collection of acts and laws passed in 1996 in the US regarding economic espionage shows the measures the legislators are taking in order to protect business and economic secrets in real or virtual space. On that basis, economic espionage can be defined as gaining wealth and benefit from external resources either via instrumental equipment or via human resources. This act involves the damages to owners and producers of secret information related to business and trade with the purpose of increasing one's benefit. Considering the fact that in modern competitive environment, industries and organizations which are not innovative can not keep up with the competition, and since exclusive access to new innovations can lead to success, economic espionage becomes highlighted. By stealing the information produced by others and through access to exclusive news and information, economic espionage leads to reduction of research and development costs and production of innovative technologies. Exclusive news and knowledge refers to the information about resources, activities, research and development, and business policies held secretly by owners and managers whose disclosure reduces their competitive advantage and has undesirable impacts on the organization. Therefor financial and economic information is highly important. If the competitors access that information, the investment resources would be lost and all the efforts by the organization would be in vain. In order to prevent economic espionage, economic information protection seems to be the most suited way. In this regard, it is important for organizations to educate their managers and authorized personnel on this issue. Also holding workshops and seminars in order to raise awareness and warn the stakeholders about these issues is highly recommended.

Economic espionage might occur due to various reasons such as trying to compensate for technological shortcomings, fear of being eliminated from the market, or trying to have free access to free or cheap research and development. However these are not all the reasons for

economic espionage. Other reasons might be to sabotage or manipulate the existing information which could be done by replacing the information, interfering with it, or deletion of information (Arabmazar Yazdi, 2006). Disrupting the system is another instance of sabotage. Another reason for attempting on economic espionage is to obtain information about the competitors' weaknesses and strengths. For example, by obtaining information about the newest products, their target markets, production levels, and final price the competitors might try to enhance their competitive power. The competitors might also try to identify the organization's strength in order to interfere with the target market and business contracts or disclose classified information. There is no single final reason for economic espionage because the purpose of economic espionage varies depending on the purposes, types, and activities of each organization. There are diverse instances of economic espionage which could easily be prevented by vigilance and implementation of information protection in financial and economic systems.

3. Methodology

Methods of economic espionage are generally divided into espionage by exploiting human factors and espionage using technical and technological equipment. Espionage using human factors refers to methods that deal with direct presence and intervention of human, while espionage using technical and technological equipment refers to methods which employ certain technical devices and instruments. There are various ways to attempt on espionage such as infiltrating the competitor's systems, undercover interviews, visiting the production line disguised as an ordinary visitor, exploiting collaborative research projects, interacting with managers with the alleged purpose of constructive cooperation, having work contractions with the institute, espionage using computer networks, infiltrating economic information resources and infrastructural data, using the lack of technological equipment to one's own benefit and sending spies disguised as technicians, and etc. As mentioned earlier, it seems impossible to present a comprehensive model for various methods of espionage because depending on each situation, conditions and purposes and volume of organizational activities may vary.

4. Finding

Instances of economic espionage in the world of business

Here some instances of economic espionage are presented. It should be noted that the following examples are provided in order to raise awareness among managers. The instances being carried out on large scales does not mean that such acts of espionage are not carried out in small scales.

In October 1995, the newspapers reported of an act of espionage carried out by US agents during their sensitive talks with Japan in the spring of the same year. These talks were being held right at the time when US had threatened to sanction importation of Japanese luxury automobiles. Each morning, a small group of officers gave Mickey Kantor, the United States trade representative, and his aides inside information gathered by the Central Intelligence Agency's Tokyo station and the electronic eavesdropping equipment of the National Security Agency, sifted by C.I.A. analysts in Washington.Mr. Kantor received descriptions of conversations among Japanese bureaucrats and auto executives from Toyota and Nissan who were pressing for a settlement, and read about the competing pressures on Japan's Trade Minister, Ryutaro

Hashimoto (Trevorton, 2004). This is a clear example of benefitting from economic information in business talks.

According to studies, on average it takes 12 years of continuous work and 231 million dollars of investment in order to introduce a new drug into the US market. However laboratories in Thailand, India, and Brazil manage to steal the drugs formula and produce it in large scales in a matter of months. This issue costs American companies 4 billion dollars every year (Schwitzer, 2008). This example shows the importance of retention of economic information related to research and development.

Managerial solutions to confront information espionage

One of the problems before economic security of countries and organizations is the threat of economic espionage by competitors. In a situation like that, protection and retention of economic information is the best countermeasure because in the world of economic competition, even allies are seeking superiority over each other (Loventhal, 2008). This is important because obtaining nouvelle innovations and exclusive access to them is the key to improvement of production capacity and competitive advantage in the economic world (Mirmohammadi & Salarkia, 2012). An industry should be basically equipped with innovation, quality, and production power in order to be able to last in the competition. For that matter solutions must be provided for protection and retention of information as one of the ways to achieve competitive advantage. The US National Counterintelligence Executive (2008:5; 2009:5) presents two suggestions in preparation for economic espionage:

1. Providing the required infrastructure, and legal and executive background in order for timely confrontation with threats.
2. Raising awareness about the threat of economic espionage among governmental and private business community by holding seminars.

The above-mentioned suggestions are large scale solutions that can be applied to top managers and planner. These policies cannot be enforced in smaller organizations. Therefor strategies should be devised for all levels of organizational activity. Protection of financial information in small organizations is sometime more important than that of large organizations. That is because large organizations are to some extent able to recover from such adversities, however smaller organizations could not hold on and in many cases they are forced to shut down, reconstruct their networks, and regain customers' trust. To prevent such disasters the most rational solution is to educate managers and stakeholders on methods of counter-intelligence; they should learn to encounter all the issues and monitor suspicious activities. They should also pay great attention to security in virtual environment and cyber security because nowadays most of organizational activities are carried out using computer systems and in virtual space. Moreover, other issues such as information security in speech, monitoring the entrance and exit, zoning, system encryption, and knowledge of rules and regulations regarding the security of economic information and legal solutions are among other factors which need to be taken seriously. It should be noted that the factors affecting information security are not limited to the instances

mentioned above. The issues discussed here are merely examples for better clarification of the subject.

In order for better understanding, the factors affecting information security can be modeled as below. It must be noted that this model is not fixed and unchangeable and can vary depending on the type of organization, its objectives, capabilities, volume of activities, policies, and other factors. However this model is generally suitable for providing an overview of the discussed subject.

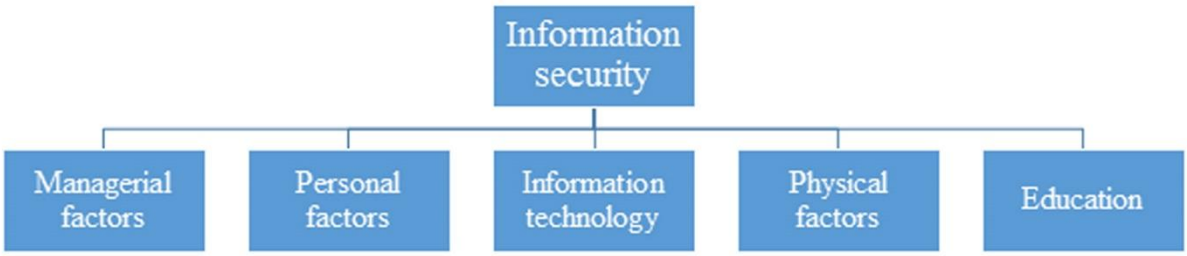

Figure 1: Information security Components

Managerial factors refer to factors that depend on the decisions of top management. These factors determine the course of action for other factors via large-scale planning. Aside from guidance and planning for improvement of information security, other solution such as system support, attention to system flexibility, preparation for reaction against possible infiltrations, and required infrastructures can also be mentioned as important matters. It is crucial for managers to pay attention to cultural factors and organizational culture in order to improve effectiveness and efficiency of the implemented programs. Neglecting this matter would interfere with the organization in the course of its main objective.

Personal factors are methods applied by individuals and personnel in order to improve the levels of information security. Protected speech, protection of documents, observation of clearance levels and classification of information, rationality and vigilance are instances of such personal factors.

Information technology refers to factors related to network, virtual and cyber space, and other similar examples which are being widely used in business environment and electronic trade. Considering its widespread applications in the organization and its vulnerability, the attempt on improving its security should not be overlooked. For instance, cyber space can become safer by means of data encryption, securing the networks, and using network security programs.

Physical factors refer to the physical structures required to protect the documents, resources, and other important objects. Security of documents and resources is at great risk if the physical environment does not have the necessary standard qualifications. The use of secure file cabinets and safes to store sensitive documents and construction of appropriate structures which prevent unauthorized entry to the geographical position of the organization are instance of physical security.

Education and training is an essential matter in any organization. In order to improve information security in the organization, the employees should be familiarized with security threats and dangers of neglecting security protocols through training sessions. Also, considering the fact that

technological advancement would change the methods of espionage, the regular training sessions should be held in which the personnel are educated on new methods and solutions for improvement of information security.

5. Discussion & Conclusion

A look at the discussed issues and presented examples indicate that if organizations do not value the obtained information, are not familiar with methods of information protection, and do not take precautionary measures to secure their information and limit the access to classified information then they will face serious threats. In the end, it should be mentioned once more that the best defense against information leak is to take offensive measures. Preventing such threats is much easier than overcoming the disasters caused by information insecurity. To start, methods of information protection and maintenance should be taken seriously in the organization. The solutions must be identified and taught to the employees. By implementation of security measures and regular updates, the organization can be insured against possible threats.

References:

1. Arabmazar Yazdi, M (2006).The use of expert systems in accounting education. Proceedings of the Eighth National Congress of Accounting Iran, Tehran, Mrndyz, pp. 53- 66.
2. Ariya, Naser (2001). Audit computer networks. Publication No. 152, Audit, Tehran, Corporate Audit.
3. Bolter, David. J. "Controlling Voice Studies, a Intellectual Property", Humanlic Studies, USA, Southern Illions University Press, 2001.
4. Crossler, R., Johnston, A., Lowry, P., Warkentin, M., Baskerville, R. & Qing, H.(2013). Future directions for behavioural information security research.Computers & security, 32: 90-101.
5. Daily, C. and Lueblfing, M., Defending the Security of the Accounting System, the CPA Journal, Oct. 2000, pp. 62‹65
6. Davis, C. E., An Assessment of Accounting Information Security, CPA Journal, March, 1997 :28‹35
7. Gadson, Roy et al. (2001). US intelligence in a dilemma, Translation Department of the Faculty of Imam Baqir, Tehran, Imam Baqir school publications.
8. Ghaemi, MH, Kamyab Nowroozi, R and Masoomi, J (2012).Ability to comply with the information requirements of accounting information systems and its impact on the performance of firms, publication of audit, Tehran, VOL 46, p. 61.
9. Ghodsi, SE and Salimi,E. (2013). Economic spying on Iranian criminal law. Quarterly happened, a new period of 5, Tehran, pp 109- 134.
10. Loventhal, M.M. (2008).All the secrets of the policy process, translation, Department of the Faculty of Imam al-Baqir. Tehran, Imam Baqir School.
11. Mirmohammadi, M and Salarkia, GH. (2012).Intelligence organizations and economic development. Journal of Strategic Studies. Fifteenth year. The third number. No. 57. Fall. Pp. 121- 147

12. Moosavi, P. Yousefi Zanouz, R. Hassanpour, A (2015).Identify organizational information security risks using Fuzzy Delphi in the banking industry. Volume 7, Number 1, pp. 163- 184
13. Nasheri, Hedieh (2005); Economic Espionage and Industrial Spying, Cambridge University Press.No.4, October, pages 735-752.
14. Niekerk, J.F. & Solms, R. (2010). Information security culture: A managementperspective. Computers & security, 29(4): 476-486.
15. Ozkan, S. & Karabacak, B. (2010). Collaborative risk method for informationsecurity management practices: A case context within Turkey. InternationalJournal of Information Management, 30: 567-572.
16. Porteous, Samuel (1994); "Economic Espionage", Intelligence and national security, Vol.9,
17. Post, Jeffrey. W.The Secrets of Trade Secrets, Protecting Your Company's Trade Secrets and Protecting Your Company Against Trade-Secret Claims, Privacy & Data Security Law Journal. 2005.
18. Pourheidari, O. (2006). Characteristics important information related to strategic decisions and their role in the design of accounting information systems. Journal of Accounting Research, (4), Tehran, pp. 10-17.
19. Rahbari, E. (2009). Trade secret rights, Tehran, publisher side.
20. Rajab Dorri, H. (2014).Place and importance of accounting information systems in the organization. Proceedings of the Third International Conference on financial management and investment accounting, Gorgan.
21. Safaei, A. (2004).Network security, Tehran, Danshprvr, first printing
22. Sajadi, SH and Tabatabai Nejad, SM. (2006).Accounting information systems. Ahwaz Chamran University Press.
23. Schwitzer, P. (2008).Friends Spyware, Translation Department of the Faculty of Imam Baqir, Tehran, Imam Baqir school publications.
24. Trevorton, G.G.F. (2004)Restructuring Information Age, information science, translation department of the Faculty of Imam Baqir, Tehran, Imam Baqir school publications.
25. Vadiei, M and Mohammadi, J (2010). Security of information systems, accounting, audit Publication, Tehran, No. 51, pp. 90 -97.
26. yuan, T. & Chen, P. (2012). Data Mining Applications in E-GovernmentInformation Security. Procedia Engineering, 29: 235–240.