Annales de l'université de Béchar des Sciences Economiques Vol: 05, N°2
ISSN 2676–1513

Human resource: a danger or a fort to the organization?

Information security in the light of economic intelligence

DR/Ismail Bendilmi
University of Batna.
Phone number 0660421551
Email: bendilmiismail@gmail.com

DR/Fouzia BERSOULI
Center University of Barika.
Phone number: 0698844885
Email : bersouli_fouzia2007@yahoo.fr

Abstract:

The information has become included within the core of daily, personal and professional life. For the organization, the thing that makes difference between it and other structures is its ability to integrate external events and resisting them in addition to its ability to first receive and analyze signals. These skills are its competitive advantage, and for this reason, it has to integrate the so-called smart economic strategies, by adopting information and communication technologies to integrate with information and knowledge system possessed by these organizations in order to form the feature which ensures achieving competition and survival. However, the rely on these technologies opens the doors to enter unexpected risks and not known in advance which made the organizations look carefully after their information security and consider it the responsibility of all its members.

This intervention comes in order to review the most important concepts related to economic intelligence and information security, by clarifying the types of risks associated with information organization, as well as the role of human resource to facilitate its process of protection or loss, in addition the role of training and devotion to the organization.

Keywords: economic intelligence, information and communication technologies, information warfare, information security.

ملخص:

أصبحت المعلومة تدخل في صميم الحياة اليومية والشخصية والمهنية، فبالنسبة للمنظمات الشيء الذي يحدث الفرق بينها وبين غيرها هو قدرتها على إدماج الأحداث الخارجية والتصدي لها، وقدرتها على تلقي إشارات وتحليلها قبل غيرها وهذه المهارات هي القيمة التنافسية لها، لهذا تضطر إلى إدماج ما يسمى بالذكاء الاقتصادي في استراتيجياتها، من خلال الاعتماد على تكنولوجيات الإعلام والاتصال في التكامل مع منظومة المعلومات والمعرفة التي تمتلكها هذه المنظمات لتكوين الميزة التي تضمن تحقيق المنافسة والبقاء والتطور. لكن الاعتماد على هذه التكنولوجيات فتح الأبواب لدخول مخاطر لم تكن معروفة مسبقا وغير متوقعة، الأمر الذي جعل المنظمات تحرص على أمن معلوماتها وجعلته مسؤوليـة تقـع على جميـع أفرادها.

لذا تأتي هذه المداخلة بهدف استعراض أهم المفاهيم المتعلقة بالذكاء الاقتصادي وأمن المعلومات، من خلال

توضيح أنواع المخاطر المتعلقة بمعلومات المنظمة وكذا دور المورد البشري في تسهيل عملية حمايتها أو ضياعها، ودور التدريب والولاء للمنظمة في ذلك.

الكلمات المفتاحية: الذكاء الاقتصادي، تكنولوجيات الإعلام والاتصال، حرب المعلومات، أمن المعلومات.

Introduction

In a competitive environment, organizations adopt economic intelligence to cope successfully with the surrounding environment and to achieve their goals. So they need information that designs the base to find the strategic position and to form the vision. The major challenge faces these organizations is in finding true information, as they help in solving problems throughout taking decisions and developing ways of working in short time.

Information became available recently with the ICT evolution. What becomes more important is the ways of conceiving, enriching, as well as leading it to the goal. The ways of research, control and disperse of knowledge operate within an informational system that includes a set of organizational tools. These tools may be human or technological; they serve in the information management as its main supplier and responsible for providing and protecting it with the required flexibility to facilitate the interactions between the organization and environmental challenges. These systems should be protected from any attack that may harm their content. It means that the security of the organization's information is the responsibility of all team members because any of the information or data leak may cost too much, thus leading to destroy its reputation. Consequently, the protection of the information system is a long-term investment process for the organization as it clarifies the defensive side of economic intelligence.

In the light of the latter, this research paper aims to clarify the possible role of human resource inside the organization as a defensive wall or gap that leaks the organization strategic information. We would like to deal with this role in the light of adopting what is commonly known as 'economic intelligence', including the following points;

- Economic intelligence and the information and communication technologies.
- Information security and the threats against it.
- Ways of information protection and the role of human resource.

Economic intelligence and information and communication technologies

Today's organizations need to respond rapidly to the surrounding opportunities and threats due to the unexpected fast changes on the social and economic levels. The organization needs to follow innovative steps so that it could succeed in such environment. The adoption of economic intelligence and making use of ICT tools would be among the means which make its processes and activities at ease. This is why we should start by defining economic intelligence.

1- **Economic intelligence:** The concept of economic intelligence appeared as a result of knowledge economy. It is based on using ICT in acquiring,

processing and sharing information with individuals so that they could invest such information in solving practical problems.

1.1. The definition of economic intelligence:

Many researches have attempted to define economic intelligence; some of them are the following

- **Harold Wilensky:** economic Intelligence determines economic activity to produce knowledge in the service of the economic and strategic objectives of the organization collected and produced in a legal context and open source[1].
- **Henri Martre** defines the Economic intelligence as a set of coordinated procedures for processing, processing, and distribution to facilitate access to useful information and economic efficiency.[2]

Due to the necessity of adopting the strategy of developing a new product, investing in a new market, the efficiency improvement, knowing competitors, taking the right decision in time ... Etc., it requires understanding the environment which is expanding and constantly being more complex, and in this context, information is considered a basic raw material for good organization management.

However, this can be achieved only through the establishment of guarantees to protect the components and heritage of the institution under the best conditions, both in terms of time or costs, these information needed by decision makers in order to achieve their strategy and objectives.

- **Christian Harbulot** : Economic intelligence is the methodology of research and interpretation of the available information to everybody in order to activate it and know its ability ", This definition is related to open information, which makes it comply to the credibility and ethics, the identity of its agents, i.e. all administration employees participate in building a culture of information**. "**[3]
- **Alain Juillet** the senior of economic intelligence of France in 2005: "Economic intelligence is based on the protection of strategic information for all economic agents, in order to maintain the competitiveness of the economic sector, protect the economy and institutions, and promote the policy of influence." What means it includes control and protection of strategic information for all economic agents.[4]

Thus, economic intelligence is the coherent activities concerned with seeking, processing and distributing beneficial information for economic operators so that they could exploit it. Such activities are performed legally with providing all protection guarantees of the organization heritage through ensuring the best conditions in terms of quality, time, and cost. Economic intelligence should to be differentiated from vigilance which is the process of gathering information so that the strategic decision making is well performed.The concept of economic intelligence should also be distinguished from spying which is acquiring information illegally.

1.2 The significance of economic intelligence:

The importance of economic intelligence lays on its ability to make various operators and partners in the development process capable of understanding and

analyzing the working environment. It also makes it easy for them to develop their abilities and cope with variables as well as predict eventual evolutions. Moreover, they can test suitable solutions to the environment resources and thus be innovative for the sake of enhancing their performance.[5]

Economic intelligence aim: it aims to control and maintain knowledge and information due to its significance in terms of organization development. It is also related to the way information is managed so to select the most significant information to be used in the decision making. It tends to link the organization's subsystems in a unified and a comprehensive system so that the data and information streaming is controlled. In addition, it aims at coordinating the different activities so that the organization overall goal is achieved. [5]

3.1 characteristics of economic intelligence:

Economic intelligence's interest or concern is to study the strategic interaction among all levels of activity which are related to starting from the base (the internal level of the organization), to the medium level (local communities), to the national level (strategies adopted by the state's decision making bodies), to multinational level (multinational corporations) as well as international level (the state's affecting strategies). [6]

333Some major characteristics of economic intelligence:

The strategic use of information with competitive advantages in decision making.

The existence of a competent administration to coordinate the the economic agents' efforts.

The strong relations between institutions, universities and local and central administrations. The formation of affecting and pressure groups.

The integration of the scientific, technical, economic, law and political knowledge.

The confidentiality of broadcasting information with the legal acquisition.

4.1 The process of economic intelligence:[7]

- **Identifying the needed information:** it means narrowing the type information we need to be provided with. This step requires from the economic intelligence agents a good mastery of the organizational system.
- **Gathering information:** once the need of information is identified, it comes the selection of research ways. All the organization levels require certain and specific information which requires obviously identifying the info resources. Such sources would include;

*Official sources: like newspapers and mass media, databases, CDs.

*Non official sources: such sources require a personal effort to be gathered. They would include the market and the personal popularity, exhibitions, the internal atmosphere of the organization and so on.

Developing the performance of economic intelligence requires from the organization to double its caution procedures in order to protect its own information heritage through knowing and using all the legal sources available for this purpose, and exploiting the human and systematic means.[8]

- **Processing the information:** it is a vital step in the economic intelligence process. Processing the information is tightly linked to its mid-term and long term value of the organization; especially in terms of strategic decisions. Processing the information means gathering all the data to be analyzed cohesively. The value of information may be affected by different factors that may lead to its misunderstanding and influence negatively the decision making. This could happen because of the data amount and credibility, what requires on the other hand assessing, extracting, analyzing and transferring the useful and beneficial data into an appropriate figure.
- **Diffusing the information for the decision making:** it is a result of all the previous steps. The information is used within the organization as an added value. Spreading Information is like orders to be executed. It is a key for the forthcoming procedures to be taken in high qualitative way so that the aim is attained. The feedback identifies whether the information played its role in satisfying the user or not. Some strategic confidential information should be kept safe and protected.

2. Information and communication technologies (ICT):

Any sort of technology is intrusive by nature because it penetrates communities whether desired or not. This goes naturally due to the need of goods and services and the "new" goods they supply. The development of organization's memory is through the transfer and storage of information and its legacy to generations using different methods and technological means. ICT plays a key role in building the infrastructure that supports economic intelligence, and despite its advantages, it has some of the risks that organizations must regard and pay a careful attention to it.

2.1 Defining ICT: ICT is the result of combination between the technology of processing information (informatics) and communication technologies (satellites, fax etc…) for the sake of gathering, storing, and processing information of all sorts.

It may be in the following equation:

ICT= computer+ network (internet) [9]

That's why we find the information technologies are linked to such technologies. Thus ICT is a term used to refer to the fast innovations being achieved in this field. NICT may also be used as an abbreviation of New ICT.

Therefore, the term "information technology" is associated with these types of technology

(TIC) *, that refers more to the dynamics of this sector of innovations in: information technology (communication) and modern communication

(NTIC) **: to indicate further the nature of the renewable and advanced technology.

2.2 The effects of using ICT in the organization: despite its advantages, ICT may be used to violate some people or organization's privacy by getting into their files to acquire information concerning their own lives. Such violation may touch some celebrities or presidents. It represents a threat and a war waged. That's why a new term 'cyber crime' has been forged to refer to such acts as a crime. The popularity of information networks made the information security a challenge for individuals as well as organizations.[10]

3.2. Information warfare: the information warfare is the conflict that aims at information control which is deemed as an element of power in modern world.[11]

It may also be defined as the use of information systems to exploit the rival's own pieces of information or information systems. Moreover, it deals with protecting one's information against any rival's attacks which aims to harm his military and economic systems. It is not necessary that such warfare breaks out of a traditional enemy, an economic competitor may wage it.[12]

The information warfare revolves through information networks, and it does not admit time and place limits, or even the laws which stand helpless in front of it. This war takes three levels: [13]

- **Personal information warfare**: it may include attacks against individual's privacies.
- **Information warfare between organizations** : it occurs within the framework of competition more than hostility, and it is twisty by all standards
- **International information warfare**: it takes place between states, or may be waged by supranational economic factors against some states. Information warfare may be differentiated from classic wars in some points:[14]

It's known by low cost of entrance with invisible borders. It occurs via networks. Information and misinformation is the core of information conflict. It is not easy to recognize the source of attack and its leading factors and means. Losses in the classic wars may be destructive humanly and economically, whereas information warfare leads to serious if not catastrophically economic costs without with so limited and indirect human losses.

II- The information Security and the dangers it faces

Nowadays, information constitutes the infrastructure of the organizations; it enables them to perform their work. The type of information and its quantity as well as the way it is showed are the core of the decision making process within the organization. Thus, the high value of information requires good conditions of their use. The issue that needs to be taken into account is the protection of information against any illegal use.

1. **The concept of information security:** it means providing information with protection against any dangers of violation. It also includes the means and the procedures to be taken so that information is kept safe from any internal or external dangers. The security of information has been defined by researchers; the most significant ones are the following:
   - information security: "A concept that extends to the preventive and administrative procedures and measures used to protect sources (devices, software, networks, databases and individuals) from illegal and accidental infringements and interference by means of intrusion or as a result of improper or inadequate procedures used In managing these sources. "[15]
   - It is also "a set of preventive measures used both in the technical and preventive areas to preserve information, hardware and software, as well as safety procedures for specialist staff.»[16]
   - There are those who define it: "Preserving the information contained in

any information system from the risks of loss and damage or from the risks of improper use, whether intentional or spontaneous, or from the risks of natural disasters."[17]

• It is defined as a set of preventive measures used in the administrative and technical fields to protect data sources from hardware, software and data, from overruns or accidental and serial interference, and from the misuse of information resources. It is associated with measures to address the risks coming out from potential natural disasters that may result in the loss of some sources totally or partially thus affect the type and quality of information provided.

According to the points above, we can define information security as the field interested in studying the ways of protecting stored data in laptops, in addition to accessories and networks, and resisting illegal access to the stored databases.

2. The evolution of information security concept: the information security concept went through different steps as follows: [18]

- • In the 1960s, computers were the main concern for information workers. Their main focus was on how to implement programs and they were not busy with information security as they were about hardware. The concept of security was about limiting access or viewing data by preventing outsiders from manipulating devices then the term computer security appeared which means protecting computers and databases. With the expansion of computers' use and the benefits of processing large data, the interest shifted to data control and protection.
- • In the 1970s, the concept of data security was moved along with the use of simple passwords to control the access to data and the development of disaster protection procedures and the adoption of plans to store additional copies of data and software away from the computer site.
- In the 1980s and 1990s, data usage became increasingly important. Information technology developments allowed more than one user to participate in databases. This led to a shift from the concept of data security to information security. It became too necessary to preserve information and look after its integration, availability and credibility where the appropriate security procedures may contribute to guarantee the aimed results and to decrease hacking and manipulating information. IBM, the American company, was the first who set a clear definition of information security and it focused on saving data from fraud incidents, distraction or illegal logging in databases. The company noted that providing a full protection for data is not possible, however it may be possible to achieve an acceptable and appropriate level of protection.

3. **Dimensions of information protection**: The following elements must be guaranteed for any information to be adequately protected: [19]

• **Confidentiality:** This means that information is not disclosed and is not seen by people who are not authorized to do so.

• **Content Integrity:** Ensure that the content of information is correct

and true, not modified or tampered with it. In particular, the content will not be destroyed, altered or tampered at any stage of processing or exchange, either in the internal processing phase or through external illegal interference.

• **Availability**: ensuring the continuity of the information system and the continued ability to interact with information and provide service to informational sites so the user of information will not be prevented from using it or entering it.

• **Non-repudiation**: It is intended to ensure that a person who has acted in connection with the information or its sites does not deny that he or she has done so, which means the ability to prove such act was committed by a person at a particular time.

4. Threats to the information security: there are four types of threats: [20]

*Service interruption: it means any late in the commercial service or in the data streaming in the organization systems due to the viruses, for instance.

* Detector: it means any undeclared access to the information which may lead to misuse. There are a lot of undeclared ways to access computer systems through the network (internet) so anybody can access it easily and this explains how spying is common.

* Alteration or modification: it means the manipulation of information via programs, devices or even data settings itself. If a user could change numbers of financial dues or modify customers' bills, it would lead to rely on false data and impede the monetary flow especially if such gap isn't figured out early.

* Falsification: the hacker can change the content of information for his own interest or for the one who works for. Some changes may occur and may include added data to computer systems like modifying transactions and inserting new files into the database.

5. The dangers the modern system of information may be exposed to: the intended dangers are more serious on the electronic systems efficiency. The dangers may be of different sorts such as mincing and destroying the performance of computing systems which lead to disable the vital services of the organization. The other sort includes the confidentiality of the information; getting access to the information may lead to great losses. The dangers are sorted according to different norms, they include: [21]

5.1 In terms of source: the source may be internal or external;

- Internal dangers: the organizations' staff is considered as the principal source of the internal dangers as they have all the information about the systems and they know the controlling system of the organization. They also know strengths and weaknesses of the system; they can also deal with the information thanks to the access they enjoy.
- External dangers: they are represented in strangers or individual outside the organization such as hackers and competitors who try to penetrate the controlling restrictions of the system to get confidential information of the organization. Otherwise, it may be in the name of natural disasters like earthquakes, volcano, flood that may cause a total or partial damage to the system.

5.2 The doer :

- **Dangers linked to the human doer**: they can occur during the process of designing tools and information systems or through programming, testing, collecting data and inserting it into the system. They can also occur during the identification of the terms of reference.
- **Dangers linked to the non-human doer**: they include natural disasters such as earthquakes, storms, fires, hurricanes, floods and so on, in addition to technical problems of HVAC systems, etc. These dangers disrupt the operation of this equipment for relatively long periods of time to carry out the necessary repairs and recover the software and databases.

3.5. Intentionality: they include:

- Dangers out of intended actions
- Dangers out of unintended actions

4.5. Their effect: they include:

- Dangers that may lead to material or physical losses
- Logical dangers

5.5 dangers linked to the system process: they include

-input dangers.
-switching on dangers.
-output dangers.

III. The role of the human resource in the information protection

The protection of information systems against dangers is one of the tiresome and time consuming missions for the organization due to the following the reasons: [22]

- The numerous dangers that threat the performance information systems.
- The computer materials distributed to many sites that may be spaced.
- Computer devices being in the hand of many members inside and outside the organization.
- The difficulty of protection regarding the organization connection to external networks.
- The fast technical progress makes the protection tools archaic in a short period of time.
- The late detection of cybercrimes does not allow learning and having enough experience to overcome such crimes.
- The high living cost of protection.

1. The core elements of the information security system: it is better to design a control system while developing the information system where this has to focus on the concept of protection and to include all elements related to computerized information system. We may determine these elements as the following: [23]

1.1 The set of electronic devices and accessories: the fast progress of computers goes in parallel with the progress of hacking. This requires developing the staff skills of the information sector to be able to face and overcome any intended or unintended misuse.

1.2 Individuals working in information departments: The individual plays an essential role in the domain of information security and computers; he has an effective impact on the positive and negative performance of computers. Therefore, computers security requires to determine specific characteristics of employees and to set clear selection standards to reduce risks, in addition to developing plans to increase the sense of security and immunity from sabotage, Yet, it needs to review or scrutinize the personal conduct of workers from time to time and change their work sites and try not to monopolize the tasks to specific employees.

1.3 Software: Software is an intangible component and a key element in the successful use of the system, so it is better to choose computers with operating systems with high security features which can protect programs, save passwords properly and manage the operating system and communication systems. Software security should be taken into consideration when designing the system and putting its programs. This would be through developing of a number of procedures such as keys and obstacles that ensure the beneficiary cannot act outside the authorized limits, and prevent anybody to manipulate and enter the system by well determined terms of reference for reading and editing files. Thus, there are two ways to distinguish who has the privilege to get files from the one who has not: software and encrypted devices.

1.4 Network of information transmission: The local or international network of information transmission is a product of the development of communications field, because it facilitated the process of corresponding between computers and exchanging files. On the other hand, it allowed stealing and deforming information, whether from inside using viruses, or through access various communication systems. Therefore, the protection and security procedures should be taken seriously to ensure the organization safety through permanent tests and providing related inspection devices. The operating used systems should be also highly efficient and detective through designing protected systems with complex locks or codes linked to communication lines that include mainly mathematical algorithms or encrypting devices.

1.5. The sites of electronic devices and their accessories: sites and infrastructure should be given a serious importance. Based on the nature of systems and used applications, precautionary measures are taken to protect the site and protect it from any harm or attack, to maintain the source of power and regularity, to identify procedures for checking ID of logging in and out users and to record every operation takes place in the site.

Conclusion:

In the light of economic intelligence, organizations endeavor to mobilize and involve their workers in protecting information and saving their heritage, so they would be able to maintain and control their information security. As long as the common dangers are associated with the use of ICT, the organizations require employees to improve their positions and loyalty and to better the human resource policy through chasing the opportunities of economic intelligence and work on the following points:

- Creating a culture of protection and share information in confrontation with the outside world; as it goes with economic intelligence that focuses on privacy.
- Raising Awareness of information security among users and recognizing their importance and goals to maintain the organization heritage.
- Training human resources on the different applications of economic intelligence.
- Sensitization of the risks related to information security and improving properly the info-systems.
- Motivating individuals emotionally and physically to enhance their organizational loyalty and fuel their newel and creative initiatives.
- Curricula should contain topics that deal with information security awareness addressed to users and administrators of all administrative levels, maintenance specialists and information systems' managers.
- Being careful (caution) of having false information, rumor, or any sort of fiction from opposite individuals and competing organizations that get and spread unofficial information during the decisions' amendments. This is so called "information opacity" which means some organization leak false information about their future economic plan to put their opponent in a maze.

References:

odèle statique pur.[24]

[1] www.ces.fr/rapport/rapsec/R5052710.pdf, P3
[2] Massoud Delmi, Economic Intelligence and Compressive Action: Hidden Wars, Madarat, Al-Quds Newspaper, The Twentieth Year, Issue 6061, Thursday, November 27, 2008, p.15
[3]Ibid., P16.
[4] http://www.medefparis.fr/Livre_Blanc.pdf.P9.
[5] Paul Gamble, John Blackwell, Department of Information, Dar Al-Farouk, Egypt, 2003, p16.
[6] Ibrahim Bakhti, Information Technology and Systems in Small and Medium Enterprises, at the link: : http://bbekhti.online.fr/trv_pdf/TIC.pdf
[7] Yahya Al Yahyaoui, at the link: http://www.trcsr.com/detail.php?id=7
[8] Paul Gamble, John Blackwell, op. Cit., P. 38.
[9] B. Martinet, L'intelligence économique, deuxième édition, Editions d'organization, Paris, 2001, P4.
* TIC = Technologies de l'Information et la Communication.
** NTIC = Nouvelles Technologies de l'Information et la Communication
[10] Due to the importance of the subject recently, high-level seminars under the presence of experts from worldwide are being held in this area. To name just a few, there are two important conferences that are held in the United States. The first is the annual Defcom, which gather together hackers from around the world, The second one, on the other hand, is Black Hat or, where security experts gather information from the world's largest companies. For more, see Magazine pc Arabic edition, issue 10, seventh year, October 2001.
[11] P. Guichardaz, P. Lointier et P. Rosé, L'info Guerre, (Dunod, Paris, France, 1999), p 21.
[12] Hisham Suleiman, Information War The New Face of War, www.islamonline.net
[13] Ibid.
[14] P. Guichardaz, P. Lointier et P. Rosé, Op. cit, pp 21-24.
[15] http://www.saidder.jeeran.com/amn.htm.
[16]The Horse Dalal Al-Fatal, Hamir .. Information Security, Dar Al-Yazuri, Amman 2008, p.14

[17] Ibid., P16.
[18]

http://www.google.com/url?sa=t&rct=j&q=%D8%A3%D9%85%D9%86%20%D9%85%D8%B9%D9%84%D9%88%D9 % D8% A8% D8% D8% D8% D8% D8% D8% D8% D8% D8% D8% D8% D8% D8% % A7% D9% 84% D8% D8% D8% D8% D8% D8% D8% A8% D8% D8% A8% D8% % A7% D8% AF% D9% 8A% 2Bdoc & source = web & cd = 12 & ved = 0CCsQFjABOAo & url = http% 3A% 2F% 2Faoacademy.com% 2Fdocs% 2F45D0 ~ 1.DOC & ei = cTBjT_ObL8PR0QXQp5WHCA & usg = AFQjCNGPsx83zoux9hSlRvUKowMfZAmt7w.
[19] Arnason, Sigurjon Thor & Willett, Keith D., 2008, How to Achieve 27001 Certification An Example of Applied Compliance Management, Taylor & Francis Group LLC. New York, USA. P3.
[20]http://www.titmag.net.ye/modules.php?name=News&file=article&sid=545
[21]http://www.cybrarians.info/journal/no3/digitize.htm.
[22] The horse Dalal al-Fattal, op cit, p38.
[23]ao-academy.com/docs/45D0~1.DOC.PP137-139.
[24] Alexis NGANTCHOU, Le Système Comptable OHADA : Une réconciliation des modèles " européen continental " et " anglo-saxon " ?, Association francophone de comptabilité, Comptabilité – Contrôle – Audit / Tome 17 – Volume 3 – Décembre 2011, P 39.