Journal of Financial, Accounting and Managerial Studies
ISSN 2352-9962/E-ISSN 2572-0147
Vol 06, Number 03 – December 2019

OEBUniv.Publish. Co.

An analytical study of the reality of information security in Algeria Telecom- Ouargla

دراسة تحليلية لواقع أمن المعلومات بمؤسسة اتصالات الجزائر – ورقلة

PhD student. **MOKRANI Kaddour [1]*,Pr.CHERBI Mohammed Lamine[2]**
[1]University of Ouargla,Algeria, mokrani623@gmail.com
[2]University of Ouargla,Algeria, cherbilamine@gmail.com

Date of receipt: 11/10/2019 Date of revision: 02/12/2019 Date of acceptation:24/12/2019

ملخص

أصبحت نظم المعلومات داخل المؤسسات موردا مهما من موارد المؤسسة، تمدّها بمختلف المعلومات التي تساعدها في اتخاذ القرارات المناسبة، وحتى تكون هذه النظم قادرة على إنجاز المهام المتوقعة منها على أفضل حال، وجب على المؤسسة حماية هذا المورد من مختلف الأخطار التي يمكن أن تعوق سيرورته. في هذا الإطار جاء هذا البحث لدراسة واقع أمن نظم المعلومات داخل مؤسسة اتصالات الجزائر بورقلة. وقد اعتمدت على المنهج الوصفي وتم التوصل إلى مجموعة من النتائج أهمها أن مؤسسة إتصالات الجزائر بورقلة تتبع سياسات الأمنية عالية من جانب أجهزة الخوادم وعمال مديري النظام لكن بالمقابل فهي تهمل جانب المحطات الطرفية والعاملين عليها داخل الوكالات التجارية، ومراكز الإنتاج..

الكلمات المفتاحية أمن معلومات، نظم معلومات، سياسات أمنية.

Abstract

Information systems within organizations become an important resource for them, since they provide them with the different information that help them make the right decisions. In order that these systems can accomplish the tasks expected of them in the best way, the organization must protect this resource from the various risks that can hinder its functioning. In this context, this research aims to study the reality of information systems security within the Algeria Telecoms company- Ouargla. It was based on the descriptive approach and a number of results were reached, among The most important of these is the fact that Algeria Telecom-Ouargla is pursuing high security policies on the part of the servers and system administrators, but in turn neglects terminal clients within commercial agencies and production centers.

Keywords: Information security, Information systems, security policies.

* **Corresponding Author: MOKRANI Kaddour,Email: mokrani623@gmail.com**

1. INTRODUCTION

Many organizations rely on information technology in so many activities which can help in decreasing time and effort and labor use as well. Information technology becomes the basis of any organization and it has so many tools that may help in reaching the objectives and it is considered as a source of value added.

Because of the over use of information technology, there are some potential hazards because of the improvement of information daily. The misuse of information technology could have some disadvantage on the organization.

Algeria Telecom is considered as an entity that affords modern communication to their clients in all over the country. Information technology has a big role in any organization, so any imbalance in its system may cost the institution serious consequences that could have negative aspects in the organization so, the problematic that should be asked :

What is the reality of information security in Algeria Telecom – Ouargla ?

1.1 Objectif of study :

The present study attempt to recognition the risk of information technology and the precautionary measure applied in Algeria Telecom and identify if this security policies can reduce risks .

1.2 Hepothese :

According to research objective, the developed hypothese is :

H0 : The organization (Algeria Telecom) has effective security policies to reduce the risk of information systems.

2.Literature review :

There is a collection of studies which dispute the information security system , Houria Chaabane, present study about defining the dangers that threat electronic accounting information system, and recognizing the reasons behind that and the protecting procedure. That should be used to face these risks. This study opt for the descriptive analytic method; the sample of the study is 12 banks in GAZA and the results of the study are banks rely on auto system with a few employees that are specialized in technology information in addition the systems that are related to internet. These employees should have their passwords and directing the information (Houria Chaabane Mohammed Cherif , 2006) in another study,Fatma nadji recognizing the relationship between the security information system and the creative level of employees and its effects on the contributed companies in Oman's Bank. The sample of the study is three(directors, internal auditors and external ones). The results of the study that there is some risks of environment with accounting information system. The risks of inputs if information system, operating data. The outputs of accounting information system (Fatma nadji El Abidi , 2013); in the telecommunications environment Ghamen El Otaibi, has present study is recognizing the relationship between information system and the level of creativity in telecommunication company of saudia Arabia . some thought that there are some tools and styles for practicing information system have some boundaries on employees that kill spirit of creativity . this study used the descriptive method by using a questionnaire as a tool for a sample of employees of selling in big parts (599 employees). The results of the study that employees agreed about the reality of information system and they have the creative spitiy and there is a strong relationship between information system and the creative spirit of the employers (Ghanem G. Al Otaibi, 2013), to evaluating the role of telecom organization facing security risk in social media in saudia Arabia, saad ben abdelhadi, present study using the descriptive analysis method and questionnaire as a tool for collect data of the study (all employees of saudia telecom) the results of this study is the lack of employees who are specialized in the field of accountant security and information and it turns out that most of the sample of the study are people who work in administration also the lack of giving advices regarding the risks about using social media (Bin Gligham, 2014).

3. Information Systems

This chapter handles some definitions that are associated with information, definitions, its objectives, its elements and its principales.

3.1 The definition of information systems

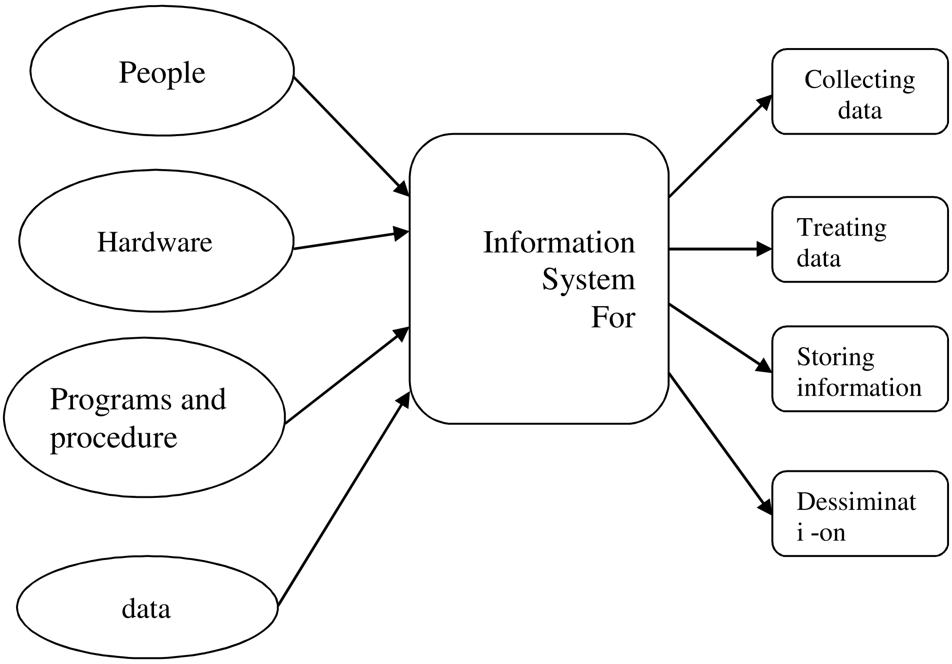
Information systems is considered as the most interesting strategy in any organization, due to most important resources of the company; there are so many definitions of this systems :

It is an organized collection of sources; physical, programs, human, data procedures, that allow to collect and treat information as (data, text, pictures and audio, …etc) (Bourliataux et al.,2008,P6).

In another definition, it is a collection of people, procedures and sources for collecting data by transforming and distribution it all over the organization (Allal-Cherif et Dupouet, 2014,P1).

It is a system that contains some parts (data, people, equipments and procedures) and work consistency via a collection of operations(collecting, storage treating and analyzing) a view the outputs and the results (report, shapes, drawsamed and shames) by providing the results in a way that support decision making and allow them planning and controlling the organizations activities (Lounis,2011,P12) .

Fig.1. Contents of information system.



Source : Reix and Fallery, 2011, p : 5.

The shapes is about the contents of information technology and its objectives, which contains from people whether users os specialists in supporting information system, and it contains hardware (machine and tripodes) then programs and procedures and this content is intangible, finally data contains files related to each other, therefore these contents react to each other for collecting data, treating data, storing data and dissemination data.

According to the previous definitions; information systems is defined as an interaction between people, hardware, programs and data by following some procedures that allow to : collect, treat, store and disseminating information inside the organization in order to make the right decisions in very activity of the organization.

3.2 Objectives of information systems :

Information system has some objectives such as (T. Al-Sudairy, 2012,23) :

- Improving effectiveness in a way correct;
- Improving efficiency : using things right in order to obtain good results and reaching the aims that have been planned;
- Easy switching : using information system for using activities effectively;
- Increasing accuracy information : very accurate information;
- Improving productivity and the quality of the product;
- Decreasing costs by providing information that may help in decision making;
- Make a connection between Clients and company via data collection;
- Increasing added value: to measure the information value with covering the benefits of every single information.
- Decreasing time while collection data.

3.3 The Principles of information system :

In any organization the information system contains some principles such as: inputs, treatment, controlling and environment that surround this information system.

3.3.1 Inputs : it is a collection of data coming from communication channels and from internal and external resources or from the system because some parts of its outputs ad an input in order to feed the system(Ta'iy,2002,P44).

3.3.2 Treatment : treat the coming data by some operations for producing outputs(Elhoush, 2007,P95) .

3.3.3 Outputs : Inputs can be transferred to outputs via some treatment operations or can be used as new inputs in the system.

3.3.4 Feedback: after evaluating the operations by the flow of information and data that may help in decision making which is considered as a sign of future performance besides correcting the system by modifying some principles in order to eliminate the errors and rise the performance.

3.3.5 Controlling : measuring the performance and using the operations that help to reach the aims that have been planned so controlling is measuring and evaluate inputs, operations and outputs to make sure that the system is making its part regarding the objectives that have been planned, so if there are some deviations, the system should make some adjustment at the level of inputs, operations and treatment in order to reach the planned objectives .

3.3.6 The environment: the environment can affect the organization and exporting its outputs after using it which means that there are a certain strong relationship between the organization and the organization each one affect the other positively or negatively .

3.4 The contents of information system :

Information system contains some contents that can be used in receiving the data resources and transferring it to final products in as an useful information starting from inputs, working, outputs and controlling (Elabd & Elkordi,2003,P30):

3.4.1 Hardware: Using tools in using information

3.4.1.1 Calculator System: Including central unit and secondary storing tools.

3.4.1.2 secondary Hardware : the mouse, keyboard, screen and printer .

3.4.1.3 Media : contains all tangible objects on which data is recorded, such as paper, optical and magnetic disks.

3.4.2 Programs : contain all working information

3.4.2.1Operation systems : Operation systems of operation, decision support or expert systems , windows is considered famous Operating system all over the word, there are other systems Unix, linux , Solaris…etc;

3.4.2.2 Application;

3.4.2.3 Procedures.

3.4.3 People: people are considered as an essential part in any information system because people are allowed to analyse, plan programs and directing the activities in ordre to be more beneficial on the company, however peole can be devided in two categories :

3.4.3.1 End users : are people who use the system directly or use the outputs by others accountants , selling people, engineers, Directors and customers.

3.4.3.2 The Specialists: they are people who evaluate and use the system concerning all system's analyst, developers, system operators.

3.4.4 Database : the organization mainly focus on data as a value added after operating all these information to become an essential data, and to manage the data to be more effective to all end users inside and outside the organization.

3.4.5 Networks: such as Intranet and extranet are essential in all types of organization whether for trading or E-business.

4.Information system security:

It is about some policies and practices that should be applied in the organization in order to discuss the movements of activities electronically via networks with a reasonable and confirmed degree of security, this security is applied on all the activities and the movements and electronics storings on business firms and clients or any other person that maybe under the risk of break thorough (ElHammadi,2013,P13).

Other definition, Information security are some procedures and measures that are used in field of administration or in the technical field in order to protect the data sources (hardware, software, data, people) from excesses and overlaps as a result of wrong procedures in managing these sources (Sadek & Fattal, 2008, P11-12).

Based on these definitions, we proposed that Information system is about some procedures and policies applied on the components of information system in order to be protected from potential hazards.

4.1 The elements of Information Security :

The strategy and the objective of information security in order to guarantee that elements are available for any information to be well protected enough.

4.1.1 Confidentiality : means to make sure that information are supposed to be covered only by reliable people, those who need it under appropriate circumstances(McCumber ,2004, 32).

4.1.2 Integrity : means to ensure that the message has not been modified in transit and is secured during transmission (Alhassan, Adjei-Quaye, 2017, 103) and make sure that the information are valid and not supposed to be messed with, by the safety of the contents in any phase of treatment or exchange whether in internal treatment with information or inappropria l interference .

4.1.3 Availability : is to make sure that information system in order to be able to interact with information and propose services for information websites so that the users of information are allowed to access these sites (Kedaifa, 2016,P166).

4.1.4 Non-repudiation : is to guarantee that the person should never deny any behavior that affect negatively on information (Kedaifa, 2016,P166) and it is supposed to give more details of any behavior that affect negatively by giving precise information (person, place, time, …etc) (Abdelkader,2011,P50).

4.2 The contents of information security :

The contents of information security are devided into (Sadek & Fattal, 2008, P 21) :

4.2.1 people security and administration security : are some procedures used to protect the security of accounting centers and people risks. Controlling the access of people and using magnatic credit cards.

4.2.2 The security of information and documents in accounting centers : documents and electronics supports (CD, Flash disks, …etc) are the most secret elements, must protected in private sites and classified based on their importance and are considered as a helping tools.

4.2.3 Security of facilities : this is about the security of hardware in order to save emergy, cooling, firefighting means and every tool related to environment.

4.2.4 Security of Hardware Telecommunications: Telecommunication is the basis of networks so that it should be protected, secure telecommunications lines, hardware telecommunications such as routers, switches and protect it from breakthrough and spying.

4.2.5 Security of operating systems and software: the organization take some procedures and substitute security to make sure that operating system and software are safe in order to acquire some defensive styles against any interference, among these procedures are passwords, permissions, authentification and backup . virus are considered the most dangerous enemy for any operating system and software, these virus may destroy the software, spying on the application so, the organization should have original antivirus versions.

4.2.6 Security of Hardware : it is the procedures to secure hardware such central unit, printers CD readers …etc.

4.3 Designing protection system :

for designing any system of protection should applied following steps (Elhamami & Alani, 2007,P42-45) :

4.3.1 threat identification : the first step is to identify the threats which can be affect the information systems, this operation can help to prepare the right way face it.

4.3.2 Information security system cost : the value of data has a major in designing system, when the value is precious the system can be more complicated .

4.3.3 Prevention actions: use some procedures and substitute to prevent stealing or destroying information, protecting in order to create some systems against fire, electric systems.

4.3.4 Detecting system : security system must have mechanism able to detecting threats in order to eliminate it .

4.3.5 Deterring: security system must have deterring procedures to punish all act (caused by persons) , organizations can concept its own deterring procedures .

4.3.6 Correcting the system: the necessity of recognizing the weak points of the system and trying to correct it in a good picture. Based on there is no perfect system without any weak points so the system should examine it to discover the weak point in order to be treated.

4.3.7 Destroying and rebuilding: when the security procedures failed in defeating the threats so. The only way is to redesign the security system by taking some new security system work on prevent any danger.

5. The Method of The study : using steps to the practical study :

5.1 Sample of the study : the study use Algeria Telecom in ouarlga as a sample of study, selecting 100 employees of information system where end users or support employees.

5.2 Analysing the result of the questionnaire : distribute 100 copy of a questionnaire anf get back 90 responses (90%), the result of the study according SPSS software Version 22.

5.2.1 Measuring validity and reliability of the study sample :

Table 1. alpha cronbach result

		Dimensions	**Nbre of paragh.**	**Alpha value**
Security policies	First	Confidentiality and reliability	4	0.806
	Second	Integrity	4	
	Third	Availability	4	
	Fourth	Non-reputation	4	

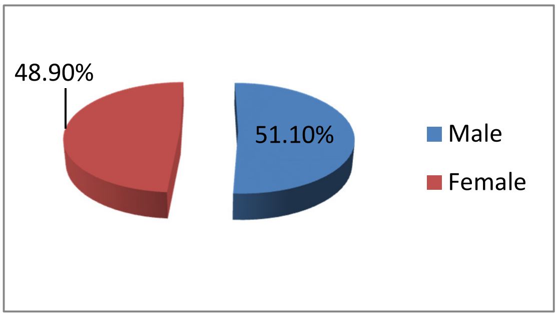
Source: researchers using SPSS V22.

The value of alpha cronbach shows that the responses of the sample acceptable it = 0.806.

5.2.2 Analysing the sample :

5.2.2.1 According to sex :

Fig 2. Disturbing sample according sex

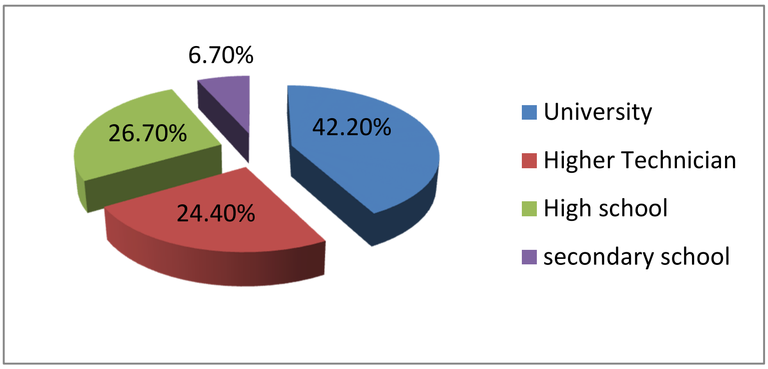


Source: researchers using SPSS V22.

The results show the sample was quite similar according this distribution .

5.2.2.2 according to the academic level :

Fig 3. Disturbing sample according Academic level

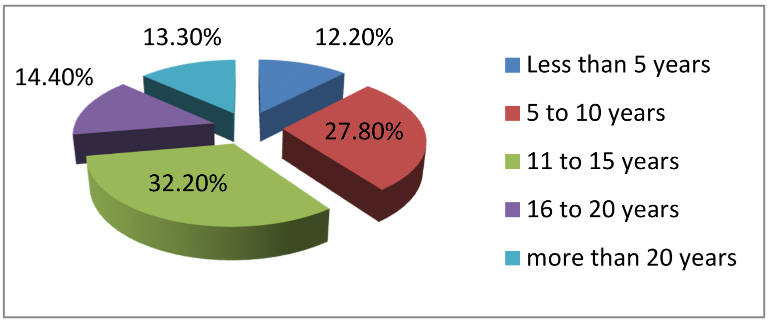


Source: researchers using SPSS V22.

The results show that most of elements of the sample have university diploma then the high school level, then higher technician and then secondary school level which are few because the organization is active in vital field and technology so that the organizations opt for higher qualities.

5.2.2.3 according to the experience :

Fig 4. Disturbing sample according experience

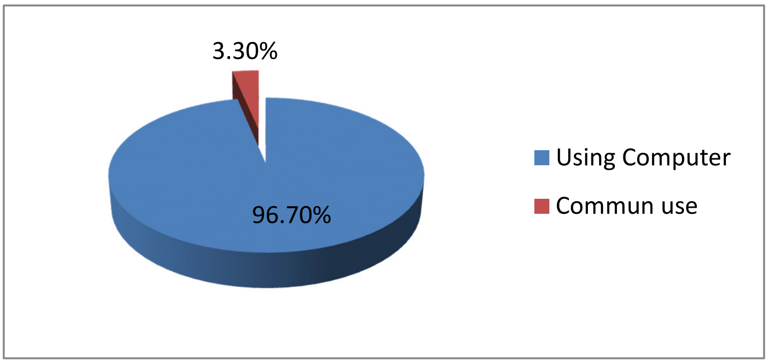


Source: researchers using SPSS V22.

Most of the sample are people who have Medium experience between 11 to 15 years that show organization is young, then people who have a new experience between 5 to 10 years, the rest of the sample are so close each other in terms of percentage.

5.2.2.4 Information System in the organization :

Fig 5. Disturbing sample Information System



Source: researchers using SPSS V22.

The sample show that they are aware with information system relying on computer otherwise only few said that information system is a combination between handy work and auto work .

5.2.3 Measuring the Direction of the members of the sample toward the security policies:

Most of the sample are people who have Medium experience between 11 to 15 years that show organization is young, then people who have a new experience between 5 to 10 years, the rest of the sample are so close each other in terms of percentage.

Table 2. Measuring opinions of employees

Security policies		Scale	disagree	medium	agree	Arithmetic mean	Standard deviation	Direction
1	Insert information after getting agreed by the head	Rep.	9	32	49	2.44	0.672	Agree
		Rate	10	35.6	54.6			
2	Make the employees aware about risks of IS	Rep.	19	29	42	2.26	0.787	Medium
		Rate	21.1	32.2	46.7			
3	Employees benefit from training when System was updated	Rep.	4	24	62	2.64	0.567	Agree
		Rate	4.4	26.7	68.9			
4	The place of converged network is secure, only qualified person can access	Rep.	15	22	53	2.42	0.764	Agree
		Rate	16.7	24.4	16.7			
5	Installation of antivirus and update	Rep.	24	33	33	2.10	0.794	Medium
		Rate	26.7	36.7	36.7			
6	Access to internet was controlled	Rep.	16	20	54	2.42	0.779	Agree
		Rate	17.8	17.8	22.2			
7	The network contains a firewall to prevent from attacks	Rep.	8	31	51	2.48	0.657	Agree
		Rate	8.9	34.4	56.7			
8	Only original version of software was allowed	Rep.	13	30	47	2.38	0.728	Agree
		Rate	14.4	33.3	52.2			
9	Network maintenance periodically	Rep.	18	40	32	2.16	0.733	Medium
		Rate	20	44.4	35.6			
10	Make backup copy for data	Rep.	5	35	50	2.50	0.604	Agree
		Rate	5.6	38.9	55.6			
11	Specialists intervene efficiently to repair any malfunction	Rep.	9	37	44	2.39	0.665	Agree
		Rate	10	41.1	48.9			
12	Hardware change periodically to be updated with latest technologies.	Rep.	11	42	37	2.29	0665	Medium
		Rate	12.2	46.7	41.1			
13		Rep.	15	44	31	2.18	0.674	Medium

	Employees change passwords periodically	Rate	16.7	48.9	34.4			
14	IP address was declared to permit get access to the SI	Rep.	8	17	65	2.63	0.644	Agree
		Rate	8.9	18.9	72.2			
15	Any access operation to the system was registered	Rep.	3	16	71	2.76	0.504	Agree
		Rate	3.3	17.8	78.9			
16	PC was protected by passwords	Rep.	11	35	44	2.37	0.694	Agree
		Rate	12.2	38.9	48.9			
						2.35	**0.537**	

Source: researchers using SPSS V22.

5.2.4 Results and discussions :

According the table it turns out that total arithmetic mean for the sample =2.35, the sample agree that there are a security policies by the organization.

The sample agree that the operations named by the person who did the treatment and he is not supposed to deny which is an essential part of information security and he is agreed about formation and training after every updates in order to make an interaction between the employees positively, there are some procedures used in declaration operation IP, protecting the used computers even if the employee try to have access to non declared computer so who won't be able to have the access to this type of computer, among the procedures in the organization, the reserve copy (backup) operations that may help in recovery system in case receiving a threat could cause losing copy that essential in information system, also there is firewall inside the organization that may prevent attacks on the company, controlling entering information by the head chef that allow participating taking responsibility, according to the questionnaire, it turn out that the organization has specific places and secure for system hardware, this procedures help in isolating tools in many external threats that may affect its performance, the results show that the organization never allow access to websites only a few of them, this procedure may help to identify some bad activities, and the operations of network repair with a medium competence, this may cause risk on network maintenance, and there are not network periodically maintenance but only interfere in case of a problem, this procedure cause a damage in information system. the organization prevent installing unlicensed software, also protecting computers with passwords but noticing that the employees don’t care about changing the password periodically which have a negative effect on the system such back through, the organization doesn’t make periodically updates to computers, which affect the employee’s performance because their performance associated with the performance of the hardware, and it does not make awareness campaigns about the risks of information systems, this procedure affect negatively in safety procedures inside information system.

To sum up the results and as a test of hypothese H0, according the global arithmetic mean for the sample which is 2.35, the company has not effective security policies, it turn out that Algeria Telecom Ouargla fellow some security policies especially that related to network, imposing some procedures to protect these hardware wether hardware insurance and insure their places, otherwise the organization ignore awareness side of the employees regarding the system, also making a maintenance of terminals such as the commercial employees in commercial agencies or production centers, in order to be able to fill the gap, the organization should take care about their employees who work in the system and taking care of system managers .

6. Conclusion

The System inside the organization considered as an essential part for every activity, so the organization ought to protect the system from danger, by applying some procedures and policies. The organization need to be more active not only providing structures and programs but it should invest more in human resources by doing some periodical formation and training that are beneficial on employees who work on information system and it is better to do some awareness campaigns concerning risks .

The Appling of these operations positively, it could help in providing a secure environment to the organization’s resources so, the development of technology, the organization needs to be in touch with the development of technology in order to be close to the external environment.

7. Bibliography List :

1. Elhoush, Aboubaker Mahmoud .(2007). Systems and networks information. Egypt: University culture foundation.
2. El hamami, Alaa hocine, Alaani, Saad Abdelaziz.(2007). Technology of information security and protection systems. Jordan: Dar Wael.
3. ElHammadi, Ali Hocine Ahmed.(2010). Proposed model for managing information and communication security in a networked environment. Jordan: Magister thesis Middle East University.
4. Labed, Djalal brahim, el kordi, Manal .(2003). Introduction in Management Information Systems. Egypt: elder elgamaya.
5. Sadek, Dalal, El Fattal, Hamid Nacer .(2008). Information Security. Jordan: Yazori publishing.
6. El abeidi, Fatma Nadji .(2012). The Risk of Using Computerized Accounting Information Systems and its Impact on the Efficiency of Auditing Process in Jordan. Jordan: Magister Thesis Middle East University.
7. Al Otaibi, Ghanem G.(2013). Information systems security and its relationship to the levels of creativity of workers in the STC, Magister Thesis. Saudia Arabia: Naif University.
8. Abdelkader, Hoida Ali .(2011). management information systems theory and application.Sudan: Djinan Publisher.
9. Cherif, Houria chaabane.(2006). Risks of electronic accounting information systems : An applied study on banks operating in Gaza, Magister thesis. Palestine–Gaza: The Islamic University.
10. McCumber, John.(2004). Assessing and Managing Security Risk in IT Systems: A Structured Methodology. USA: CRC Press.
11. Kedaifa, Amina.(2016). Strategy of Information Security, *abaad iktissadia*. Vol 6.(N° 01).
12. Lounis, Nadia.(2011). The impact of information and communication technology in activating the business of enterprises, Magister Thesis, Algiers 3 University..

13. Al-Sudairy, Mohammed Ahmed T. (2012), Management information systems. Saudia Arabia King Saud University.

14. El taai, Mohammed Al fardj.(2002). The complete encyclopedia in computer management information systems. Jordan: Zahran publisher.

15. Alhassan, Mohammed Mahfouz, Adjei-Quaye, Alexander.(2017). Information Security in an Organization, *International Journal of Computer (IJC.* Vol 24, (N° 01).

16. Oihab, Allal-Chérif, et Dupouet, Olivier.(2014). Optimisez votre Système d'Information « vers la PME numérique en réseau », France : Afnor,Saint-Denis.

17. Bin Gligham, Saad Abdulahadi.(2004). Assessing the control role of the communication and information technology commission in reducing the security risks for the uses of the social networking, Naif University Saudia Arabia: Magister thesis.

18. Bourliataux, Stéphane, Gallitre, Cyril & Roy, Yvers (2008). Information systems for management. France : Dunod.