

**The effectiveness of information security on improving the  
quality of decision-making**

**Dr: Amr Ibrahim Awad Al-Shora**

**Lecturer of Computer and Information Systems**

**The Higher Institute of Management and Information  
Technology, Kafr El-Sheikh**

**Abstract:**

The study aimed to identify the effectiveness of information security in improving the quality of decision-making. The study is based on information security and its effect on improving the quality of decision-making. It was conducted in the General Directorate of the Ministry of Finance in Kafr El-Sheikh Governorate in 2018. The researcher used a questionnaire to identify the effect of information security on improving the quality of decision-making. The study sample consisted of employees in the Real Estate Publicity Department; some of them were from Real Estate General Taxes Department and Real Estate taxes Department in Kafr El-Sheikh. The sample was 65 employees. The most important results of the study were that there is an effect of information security on improving the quality of decision-making. The study recommended the need for understanding the nature of threats, risks and attacks that affect

information security, the necessity of monitoring employees periodically. It also recommended the necessity of installing and extending network cables in protected places. Moreover, it necessitated using anti-virus software.

**Key words: information security / decision-making**

### **Introduction and the problem of the study**

Most developing countries suffer from the lack of a comprehensive and a national well studied strategic plan to protect the information published by them. Thanks to the amazing technological development in computer and internet programs, there has become a new type of crime called electronic crimes. This kind of crimes led to information insecurity. To fight that type of crime, a strategies and plans must be done to increase and protect information security, which help to facilitate business in a way, which does not conform to the aim of publishing that information. (Heitz & Beziat, 2016).

The safety and confidentiality of information are the main issues that require following-up and interfering by governments. But the need and demand for it increased because of the widespread use of the Internet and the dependence on it in all aspects of life, which required the transfer of data and information across multiple networks. The role of information nowadays is not only having the knowledge for learning, but also became more important and greater role such as decision-

making. The value of the decision depends on the value of the achieved results. As long as the logical effect depends on the aims, the value of the decision is related to the degree of its effect on achieving those aims (Donelan, 2013).

The effectiveness and efficiency of management and the extent of its ability to make decisions depend on the adequacy of the information and its good usage. So that the accessible, accurate and sufficient information is required to increase the effectiveness of the decisions (Alenez, 2013).

As previously discussed, there is a bad need to improve the process of the decision-making process in the government in general and in the Ministry of Finance in particular. In addition, the recommendations of previous research, confirm the need for developing the process of decision-making. So this study aims to investigate the effectiveness of information security and its significance on improving decision-making. Thus, the problem of the study is formulated in the following main question:

-What is the effectiveness of information security on improving the quality of decision-making? From the previous main question, the following sub-questions are branched:

1. What are the risks and threats that affect information security?
2. What is the information protection plan?

3. What is the concept of the decision-making process?
4. What are the difficulties that face the process of improving the quality of decision-making?
5. What are the factors that affect improving the quality of decision-making?

### **The Aim of the Study:**

The study aims at identifying the effectiveness of information security on improving the quality of decision-making.

### **The Method of the Study:**

The researcher used a descriptive, an analytical method based on an opinion questionnaire to collect data.

### **Delimitation of the Study:**

The study was conducted the study along three months in 2018 in the Ministry of Finance, in Kafr El-Sheikh Governorate.

### **The Study Instruments:**

A questionnaire to evaluate the effectiveness of information security on improving the quality of decision-making. It was administered to the employees in the Ministry of Finance.

### **The Study Terminology:**

#### **- Information Security:**

Information security is the provision of the means and procedures that achieve protection from future unwanted

procedures. These events are called threats and usually lead to the loss and disclosure of confidential information (Salem, 2013).

- **Making-decision :**

It is the process of choosing among a group of alternatives to achieve one or several goals (Al-Najjar, 2014).

**The Study Procedures:**

In the light of the study problem, its aim and its delimitations, the study plan of the study is as follows:-

1. Reviewing the literature and relevant studies.
2. What are the risks and threats, which affect information security?
3. What is the information protection plan?
4. What is the concept of the decision-making process?
5. What are the difficulties, which hinder the process of improving the quality of decision-making?
6. What are the factors, which affect improving the quality of decision-making?
7. Field study.
8. Discussion of the study results.
9. Results and recommendations.

**1- Previous Studies Related to the Current Study**

Al-Ubaid, (2011) aimed to developing an advanced information system (IF) that enables the organization to reduce distances and

organize thinking through numerical calculations based on analysis and logic. Thus, IF provide appropriate information in the appropriate time through artificial intelligence information systems to face the crisis and the ability to make a decision and the availability of information to handle and manage crises according to modern scientific methods associated with e-government. The study of Ali and Etran's (2012) study aimed at evaluating the effectiveness of public opinion measurement methodologies on making a decision. The study was performed on an intentional sample of experts in public opinion measurement studies consisting of 58 items. The technique of collecting the information is a questionnaire that covers all the study dimensions. The researcher interviewed 58 experts who have awareness and interest in measurements of public opinion. The study established a set of methodologies on making a decision according to establishing a list of possible solutions and options, setting a timetable, determining who is responsible for decision-making, collecting information, and estimating points of weakness and strength. The study Al-Saheb (2013) highlighted the importance of information security at universities and the causes, which make universities more vulnerable to threats. The study concluded that there is a need to have a document of information security policy at universities followed by a set of procedures and instructions to adhere to them by not committing Computer crimes.

Al-Shujairi (2014) aimed to investigate the important difference

---

between political decision-making as a subject for analysis according to a systematic model that is carried out in natural conditions and decision-making in a period of crises, where it was revealed through research the great role played by the information flow in decision-making in a crisis in a world has a great role of information. The study found that information has been and remains the main variable in the decision-making process of the crisis, which cannot be ignored by decision makers when they prepare to make their decisions. Dakhil and Talha (2016) also described the importance of information security and clarified the most important problems and threats which face information users in addition to addressing ways to protect information by developing a strategy for this and stresses on the necessity of continue to spread awareness and training in this field.

In spite of the valuable contributions made by previous studies, these studies did not deal with the effect of information security in improving the quality of decision-making according the e-government by application on the Ministry of Finance Website.

## **2- Threats, Risks and Threats that Affect Information Security:**

In general, the risks and threats are classified as follow:

- **Violation of physical protection:**

It means the attackers search in the institution waste and

---

abandoned materials in search of anything that helps them to penetrate the system, such as papers with passwords or computer outputs that may include useful information or discs that are discarded after replacing them or notes (Muslim, 2010).

- **Computer viruses:**

Computer viruses are programs designed to penetrate the work of the computer by copying, corrupting or removing the data recorded on it or copying themselves to other computers or over the Internet and this often causes slow operation of the device and may cause other problems (Wrighton, Reiter 2016).

- **Hackers and Crackers:**

The word hackers means an innovator of information systems and software. The hackers are people with a high level and technical skills. They can decode the codes and gaps that harm many institutions and networks. They can be professional programmers who are able to create programs and are able to solve the Software problems in the computes in all its systems (Abdel-Moneim, 2015), while the word Crackers means breakage or cracking and its general meaning is ruining, messing up, tampering and smashing. They are a group of criminals who are able to penetrate any network or computer device (Al-Eifah, 2014).

**3- Information Protection Plan:**

The plans for facing risks start from the stage of the necessary



technical, administrative, informative and legal procedures, and the stage of the analysis procedures for the nature of the risks that occurred, the reason for their occurrence and how to prevent them from happening later. Finally the recovery procedures and returning to the normal situation (Nowicka, 2014). To secure and protect the data we use the following set of methods:

### **A- Physical protection methods:**

They are represented in choosing the appropriate place and equipment to maintain security. To achieve this level of protection, we must do the following: (Abu Kamil, 2011).

- A closed room allocation to keep the network server devices in case they are placed in central rooms.

- Choosing the cables that are the most protective to the information represented by optical fiber cables.

- Installing the network extensions and cables in protected places that are not exposed to the access of non-specialists.

- Providing site-monitoring tools, such as CCTV.

### **B-Controlling access to the network and make its resources available.**

This can be done through the following:

- **Availability of participation level:**

An identification name and a password are specified for each

available source for sharing on the network. Every recipient who wants to access this source uses the same name and password. The disadvantage is that the user should remember multiple passwords, each of which is specific to one of the sharing sources (Lee, et al., 2014).

- **Availability on the user's level:**

The user must follow the rules, which are used to protect the password to ensure that it is not disclosed by others, and among those rules: changing the password regularly at least every 30 days and avoiding using easily expected words. . (Christa & Mark, 2015).

- **Data Encryption:**

Encryption is defined as the process of forming data using a specific algorithm by which it becomes unreadable until the algorithm is used to decode it. The data is usually encrypted before being sent over the network in order to ensure the integrity of its access without exposing to any spying or misrepresentation of its content, provided that the code is deciphered by a receiver message using the decode key. (Ayed, et al , 2015).

- **Using a firewall:**

The firewall is a program to protect network resources from the users of other networks. It is used in the case that the network is linked to large networks to prevent external users from

accessing network resources and private data. (Johnson, 2015).

- **Antivirus software:**

Viruses can be divided into two main types: the macro virus and the operating sector virus, and each of the two types differs in the way it infects computers. It also differs in the way it affects them. The macro virus is a small program written using an internal programming language for applications such as Visual, it copies itself inside the files created using application programs. The macro works on opening, closing the file, on saving a file, or while the program is running. The operating sector virus, which does not need, like the previous type, files to enter the device as the device becomes infected with the virus on trying to run it through an infected disk and on turning the computer on, the virus is transmitted to the device memory (Abolamady, 2017).

- **Using anti-virus software:**

Many companies produce anti-virus programs such as, Symantec, Command, MacAfee and others. These programs work as follows:-

- Checking the computer memory when it starts up searching for any viruses.

- Checking the storage disks searching for any viruses, on finding some, they are removed or the infected files can be deleted.

- Checking the files, whether they are available for sharing, transmitted via the Internet, or sent via e-mail, to ensure that they are free of viruses, alerting if there are any, and providing protection against them.

- The Continuous checking to the system to ensure it is free from Virus. (Ying & He, 2017).

- **Backup:**

Data backup achieves this appropriate level of protection. By backup, copies are created that are saved either at the same workplace or outside, and are updated regularly to ensure the least amount of losses in case of losing the original data, and copies are made daily, weekly or monthly according to what suit the work (Ali, 2015).

- **Protection by persons (employees)**

Employees are considered are the main element that may harm information and threaten its security, whether intentionally in case they want to offend the organization for any reason, so the following procedures should be done:

- Assigning passwords for employees taking into account specifying the authority of each employee.

- Choosing the employees carefully, especially those who deal with sensitive data and who are given high authority.

- Training staff well in order to avoid many of the problems

that the network and its resources might face because of the poor technical level of workers on it. (Mwesigwa, 2013).

#### **4- The Concept of Decision-Making Process.**

The decision-making process in the past depended on guessing and forecasting, and on the experiments and experiences of the decision-maker. Nowadays, the decision-making process follows scientific and systematic methods. The decision-making process is defined as the process of choosing the best alternative from a set of alternatives. The information supports a quality process. (Fico, 2017).

#### **5- The difficulties that encounter the process of improving the quality of decision-making.**

According to Kediri's, et al, (2013), the most important difficulties related to the decision-making process are:

- The scarcity of a single or correct solution to the problem presented. Usually, there may be more than one acceptable solution.

- Not delivering the decision to the officials in the appropriate time and manner.

- Preventing the decision, in case it was imposed by the highest ranked officials.

- The inability to define goals that can be achieved through the decision-making process.

- Difficulty in identifying the advantages and disadvantages of the expected alternatives in the environment in which the organization operates.

- Difficulties related to the personality of the decision-makers, in addition to the degree of their intelligence, experience, and their scientific, mental and physical capacities.

## **6- Factors affecting improving the quality of decision-making?**

Improving the quality of a decision made by administrative levels depends on the availability of the information to decision makers, and the decision is influenced by many factors, including: -

### **- Risk Management :**

Risk management plays an important role in the decision-making process by clarifying the situations of risk, uncertainty and trust facing the decision-maker. The risk management contributes to identifying weaknesses and strengths within the organization and the body and informs the user of the threats that the decision-maker can face, which helps to know and address points weakness, strengths and decision making at the right moment (Roberto, 2017)

### **- Quality of Information:**

Quality of information is the largest and fastest repository of

data, information, studies and reports of companies, and for this reason, information has the greatest importance in the company website and e-services (Robert & Racine, 2001).

- **Electronic Quality:**

Electronic quality means the element of predictability of the client needs and presenting them to the company. It means the different layers of data service that are provided by network sources for higher service layers with less cost. (Higher service at a lower cost) (Aldeek.2010).

- **Software Quality:**

Software is the administrative and technical mechanical brain of the computer and the company's internal and external network. It performs and helps to carry out various operations. Deals and services are usually determined in advance in cooperation between the company and the programmers for final customers (Rama, 2014).

- **Diversity of electronic services:**

The electronic services are many and varied; they cover all fields of traditional service. Therefore, these services, as Chang (2011) identified the field for electronic services ranging from commercial services, search engines, and electronic auctions to partnerships, groups.

- **Electronic Ethics:**

Electronic ethics ensures making moral business dealings, safe

---

polling, and safe browsing for companies' sites and service providers. Lack of credibility and manipulation can limit the service and reduce other quality dimensions, such as trust, reliability, privacy policy, and information protection (Taylor, 2008)

## **7- Field study:**

To collect data, the researcher prepared a questionnaire according to the following steps:

### **- Purpose of the Questionnaire:**

The aim of the main questionnaire is to investigate the effect that information security plays in improving the quality of decision-making at the departments of the Ministry of Finance. The following sub-objectives branch from the previous main objective:

1) Identifying the effect, which is played by the domain (protection of information infrastructure) on improving the quality of decision-making?

2) Recognizing the importance of the elements of the first domain (protecting the information infrastructure) to improve the quality of decision-making?

3) Identifying the effect of the (safe use of information) domain on improving the quality of decision-making?

4) Recognizing the importance of the elements of the second domain (the safe use of information) to improve the quality of decision-making?



**- Formulating questionnaire statements:**

After analyzing the metrics related to the subject of research and identifying the main domains of the questionnaire, the questionnaire statements were formulated for the independent variable in the first domain (protection of information infrastructure), in 28 items. In addition, the second domain (the safe use of information), in 20 items, and the third domain (improving the quality of taking decision) in 22 items.

**- Calculating the scale reliability.**

The reliability of the scale was calculated using the Cronbach's Alpha method, and it was found 0.8546 (see Table 1), and so, the scale is considered to be consistent.

**Table (1)**

**Alpha-Cronbach Questionnaire Consistency**

<b>N</b>	<b>Domains</b>	<b>Cronbach's Alpha</b>
1	- Information Infrastructure Protection	0.791
2	- The safe use of information	0.816
3	- Improve the quality of decision-making	0.857
<b>Total reliability score</b>		0.8546

**- Study sample:**

The sample of the study consists of employees in the real

---

estate publicity department and general real estate taxes in Kafr El-Sheikh Governorate, and the study sample was selected by the purposeful technique. The researcher was allowed to contact the subjects for the questionnaire, and the sample size was 65 participants (See Table 2), the response rate was 81% where the number of responses was 240, questionnaire response rate was 80%. This is an acceptable ratio to conduct statistical analysis.

**Table (2)**

**Distributed and Received Survey Forms**

N	Domains	Distributed forms			Responses ratio
		Distributed	Completed Received	Uncompleted	
1	- Information Infrastructure Protection	80	65	15	81%
2	- The safe use of information	80	65	15	81%
3	-Improve the quality of decision-making	80	65	15	81%
Total		240	195	45	81%

**-E-Statistical analysis:**

After coding the data and computerizing it, the researcher analyzed the data provided in the survey list using SPSS version (19) program.

**-F- Hypotheses of the Study:**

**The main hypothesis stated that:**

There are no statistically significant differences between the effect that information security plays on improving the quality of decision-making at the (0.05) level.

The following main hypothesis is subdivided into the following sub-hypotheses:

1- There are no statistically significant differences between the effect of (Infrastructure Information Protection) domain plays on improving the quality of decision-making at the (0.05) level

2- There are no statistically significant differences among the elements of the first domain (protecting the information infrastructure) on improving the quality of taking decision at the (0.05) level

3- There are no statistically significant differences between the effect that the (Safe Use of Information) domain plays on improving the quality of decision-making at the (0.05) level.

4- There are no statistically significant differences among the elements of the second domain (the safe use of information) on improving the quality of decision-making at the (0.05) level

**- Hypotheses testing:**

**Table (3)**

**Estimated Responses According To Questionnaire Results**

N	Response	Weighted Mean	Trend
1	Strongly Disagree	From 1 to 1.80	Strong Disagreement
2	Disagree	From 1.81 to 2.60	Disagreement
3	Quite Agree	From 2.61 to 3.40	Neutral
4	Agree	From 3.41 to 4.20	Agreement
5	Strongly Agree	More than 4.20	Strong Agreement

**-The Main Hypothesis:**

- The main hypothesis states that "There are no statistically significant differences between the effect that information security plays on improving the quality of decision-making at the (0.05) level.

**Table (4)**

**Correlation Coefficient between the Independent and Dependent Variable**

normative error for estimation	R Square	R Square	Correlation Coefficient
3.84831	0.272	328.0	0.581

**Table (5)**

**Anova Test Summary**

**Independent Variable (Protection of Information Infrastructure, Safe Use of Information) Dependent Variable (Improving Decision-Making Quality)**

	Sum Of Squares	Df	Mean Square	F	Sig.
<b>Regression</b>	<b>231.581</b>	<b>2</b>	<b>32.819</b>	<b>5.781</b>	<b>0.004 *</b>
<b>Remained</b>	<b>638.819</b>	<b>79</b>	<b>6.182</b>		
<b>Total</b>	<b>870.400</b>	<b>81</b>			

\* Significant at the (0.05) level.

It is clear in Table (4) that the independent variables (protecting the information infrastructure) (the safe use of information), which represent the dimensions of information security related to the dependent variable (improving the quality of decision-making) by (0.581), which is a weak and covariant correlation (positive). As seen in Table (5), the calculated value of (F) was (5.781), and degree of freedom (79.2) which are statistically significant, at the level of significance (0.004) which is less than (0.05). Therefore, the researcher rejects the main hypothesis. The researcher accepts the alternative hypothesis as follows: "There are statistically significant differences between

the effects that information security plays on improving the quality of decision-making".

**- Sub-Hypotheses:**

**- The First Sub-Hypothesis:**

-- The first sub-hypothesis states that "There is no statistical difference between the effect which the (Infrastructure Information Protection) domain plays on improving the quality of decision-making at the (0.05) level."

**Table (6)**

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
<b>- Information Infrastructure Protection</b>	<b>3.749</b>	<b>0.823</b>	<b>0.417</b>	<b>2.359</b>	<b>0.0084</b>

It is obvious in Table (6) that (protecting the information infrastructure) has an effect on improving the quality of decision-making, and this effect is statistically significant, as the significance level (0.0084) is less than (0.05). Hence, the first sub-hypothesis is rejected. The alternative hypothesis which says, "There is statistical significance effect between the domain (protection of information infrastructure) and improving the quality of decision-making." Is accepted.

**- The Second Sub-Hypothesis:**

- The second sub-hypothesis states, "There are no statistically significant differences among the elements of the first domain (protecting the information infrastructure) on improving the quality of decision-making."

**Table (7)**

**Weighted Mean For The First Domain**

<b>N</b>	<b>Domain</b>	<b>Weighted mean</b>	<b>Comment</b>
<b>1</b>	<b>- Protecting the information infrastructure</b>	<b>4.182142857</b>	<b>Agree</b>

With reference to table (7), it is clear that the weighted average of the domain as a whole is (4.182142857) and Table (1) a Likert scale indicated that the general evaluation of the domain is "an agreement" and that the phrase: there are training courses for employees in the information security in the company "there is an agreement to some extent". The following phrases: The information does not reach anyone who is no longer in the company. There is supervision record that includes user activities and information security incidents. The electronic information software is subjected to continuous updating. The systems used provide automatic download service. Keeping information and classifying it according to its importance. Internet cables are secured well. I can validate the entered data. Any modification to

the data security is accepted through modifications. The information is protected by programs. Databases are available at multiple security levels. Any employee who has leaked information is dismissed and the general evaluation for these statements is an agreement on the part of the study sample.

The following phrases were rated as "Strongly Agree": The technician makes physical adjustments to the equipment. The internet can be used on my phone. Verify that the password is not revealed. The computer screen is locked manually when used. The state guarantees the integrity of the communication lines of information. The devices are maintained manually. I can get a suitable internet subscription to access the information. The systems used provide backup service. The entered information is automatically verified. The presence of electronic control to protect the electronic signature. Each employee is assigned a responsibility for information security. There are many communication companies that provide information service. Companies are developing a plan to protect information periodically. Passwords are kept confidential. I use Wi-Fi to get information anytime employees pledge not to disclose any sensitive information. With reference to the Likert scale, these statements were strongly agreed upon.

**- The Third Sub-Hypothesis:**

- The third sub-hypothesis says "There are no statistically



significant differences between the effect that the domain (the safe use of information) plays on improving the quality of decision-making at the (0.05) level.

**Table (8)**  
**Weighted Mean for The Domain**

Domain	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
- The safe use of information	3.837	0.819	0.428	2.471	* 0.0072

\* Significant at the (0.05) level

As shown in Table (8), the(the safe use of information) has an effect on improving the quality of decision-making, and this effect is statistically significant at the level of significance of (0.0072) which is less than (0.05). Hence, the first sub-hypothesis was rejected. And the alternative hypothesis which says, “The existence of the effect there are statistically significant differences between the effect that the domain of (the use of Information Security) to improve the quality of decision making” was accepted.

**- The Fourth sub-hypothesis:**

- The fourth sub-hypothesis says that “There are no statistically significant differences among the elements of the second domain (The safe use of information) on improving the quality of decision-making at the (0.05) level.”

**Table (9)**

**Weighted Mean of the Second Domain**

N	Domain	Weighted Mean	Comment
1	- The safe use of information	4.15	Agree

Table (9) indicated that the weighted average of the domain as a whole is (4,15) and table (9) displayed that the general evaluation of the domain obtained an agreement. The statements: there is a body charged of supervising the information security, the user is known about the Information Security Policy, there is a written security policy for information, Information security errors are recorded in reports, there is a record for user's activity of information security, user privileges are closed after a period of inactivity, Access to some wireless information security services is blocked, there are periodic reviews of user powers to access information security, data entry authentication for information are done according to the administrative level, and the performance of external parties is monitored when any adjustments have been done. Their general evaluation is according to Table (3) showed "AGREE". As for the statements: Information security is reviewed periodically. Each user has their own unique identity and no public accounts. there is a mechanism for reporting information security incidents. there is a periodically Back up of information. there are companies to find

out the information security vulnerabilities. Users are instructed to create a strong password. there is a system for encrypting and coding information automatically. there is security control of the information. Recruitment of employees with a security background. And cooperating with the latest companies to obtain updates in information security periodically. the overall evaluation pointed out a strong agreement.

### **8- Results:**

The study finding can be presented as follows: -

The results indicated that the security of information has an effect on the quality of decision making.

The results also revealed that information infrastructure affects the quality of decision making.

In addition, the results pointed out that information security is a relational concept that can be used to satisfy the needs of the users

Evaluation of decision making should be based of the processes and phases of taking decision and the way through which the alternatives can be evaluated.

### **Recommendations:**

On the bases of the previous studies and the analysis of the theoretical framework, the current study came out with a set of recommendations, the most important of which are:

- The need to understand the nature of threats, risks, and attacks that affect information security:

- The need to dispose of garbage and waste materials in the organization and management in an organized and periodic manner.

- Preventing flash drives or downloading unknown source programs so that the devices to avoid viruses.

- Keep the devices IP from anyone accessed to prevent hacking and cracking.

- Assigning closed room to keep the network server devices in case they are located in central rooms

- Selecting the cables that protect most information such as optical fiber cables.

- Installing the network extensions and cables in protected places that are not exposed to the access of non-specialists, so that they are not clearly visible.

- The use of shield cables to reduce the secondary radiation emerged from them.

- Securing windows and other openings in the server room, especially if they are close to the ground.

- Securing doors and other windows using automatic alarms that activate bells when anyone enters the building.

## المراجع

### اولاً: مراجع باللغة العربية:

- ١- ابو كميل، سعد محمد (٢٠١١): "تطوير ادوات الرقابة الداخلية لهدف حماية البيانات المعدة الكترونياً " رسالة ماجستير غير منشورة، كلية التجارة، جامعة القاهرة.
- ٢- دخيل، احمد نوري & طلحة، سعد عبد السلام (٢٠١٦): " اختراقات امن المعلومات وكيفية تفاديها "، طرابلس، المجلة الدولية المحكمة للعلوم الهندسية وتقنية المعلومات، مج ٢، العدد ٢.
- ٣- الشجيري، فايق حسن (٢٠١٤): " اهمية التغذية المعلوماتية في اتخاذ قرار الازمة "، الجامعة المستنصرية، مجلة السياسة الدولية، جرنال الدولي والسياسي.
- ٤- الصاحب، محمود حسن (2013): "تهديدات امن البيانات في الجامعات: البوابة العربية لأمناء المكتبات والمعلومات العدد ٣٣.
- ٥- عبد المنعم، عادل (٢٠١٥): الهاكرز " مركز المستقبل للأبحاث والدراسات المتقدمة - الأحداث الشائعة، العدد ١٢
- ٦- العبيدي، أمل محمود على & الجبوري، فؤاد يوسف عبد الرحمن & الربيعي سمية عباس مجيد (٢٠١١): " ادارة الازمات الالكترونية واتخاذ القرار "، مجلة جامعة بابل، المجلة الاكاديمية العراقية، المجلد ١٨، العراق، ص ص ٨١-٩١.
- ٧- على، ايمن مصباح (٢٠١٥): " تقييم مخاطر عدم حصانة ضمان المعلومات"، عمادة الدراسات العليا، جامعة القدس، القدس - فلسطين.
- ٨- على، عوجة & عتران، حنان محمد صدقي (٢٠١٢): " تقييم فاعلية منهجيات قياس الرأي العام عند اتخاذ القرار: دراسة ميدانية على مركز استطلاع الرأي العام بمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء"، كلية الإعلام - قسم العلاقات العامة والإعلان، جامعة القاهرة.
- ٩- العيفة، جمال (٢٠١٤): " قرصنة البرمجيات: الوضع الراهن والتحديات " البوابة العربية لأمناء المكتبات والمعلومات، مجلة علوم المكتبات والمعلومات، العدد ٣٦.
- ١٠- مسلم، منان محمود (٢٠١٠): " التحديات الامنية في شبكة الحساسات اللاسلكية" مجلة

الاتصالات الدولية، العدد ٣.

١١- النجار، حسنى زكريا (٢٠١٤): " النموذج البنائي والعلاقة بين الابداع الانفعالي ومهارات اتخاذ القرار لدى طلاب الجامعة "مجلة كلية التربية جامعة بنها العدد ٢٥، الجزء الاول.

١٢-مراجع الانترنت:

١٣- ابو لمضى، محمد (٢٠١٧): " التبعات القانونية في مجابهة شبكة البرامج الخبيثة "المؤتمر الدولي لمكافحة جرائم الإنترنت في فلسطين،

<https://hdl.handle.net/20.500.11888/13487>

١٤- سالم، حسن عبد الله (٢٠١٣): " تامين وحماية البيانات في نظم التجارة الالكترونية "

[URI: http://repository.sustech.edu/handle/123456789/8439](http://repository.sustech.edu/handle/123456789/8439)

ثانيا: مراجع باللغة الاجنبية:

- 1- Aldeek, F. (2010)."Relationship between Information Quality and Decision Effectiveness: A study in The Banking Sector in Jordan" A published thesis submitted in accordance with the conditions governing candidates for the degree of doctor of philosophy (PHD), University Ultra, Malaysia.
- 2- Ayed AB, Halima MB and Alimi AM. (2015) : "Big Data Analytics for Logistics and Transportation" By Proceedings of the 4 Th International Conference on Advanced Logistics and Transport (ICALT), IEEE, Pp311-316.
- 3- Chang .E. (2011): "Trustworthiness Measure for e-Service " [Available on: \(www.lib.unb.ca\)](http://www.lib.unb.ca)
- 4- Christa Anderson, mark minas (2015) ":Glossary of messaging and network security terms."

- 5- Donelan, R (2013): "Development and Validation of a Generic Instrument for Assessing the Quality of Decision-Making" A published thesis submitted in accordance with the conditions governing candidates for the Degree of doctor of Philosophy (PHD) Cardiff University, uk
- 6- Fico (2017):" Who Uses Predictive Analytics "analytics. Accessed 11 May
- 7- Heitz A, Beziat (2016):" A the parcel industry in the spatial organization of logistics activities in the Paris region: Inherited Spatial Patterns and innovations in urban logistics systems. Transp Res Procedia.
- 8- Johnson, L. (2015). Security Controls Evaluation, Testing, and Assessment Handbo Agree. Syngress.
- 9- Kediri's AP, Kolas VD, Nikita KS (2013):" Smart cards in healthcare information systems: benefits and limitations. In: Proceedings of 13th international conference on bioinformatics and bioengineering (BIBE), Chania, Greece, IEEE.
- 10- Lee.s , Grima.S ,Jearock.K (2014):" Design and implementation of vehicle tracking system using GPS/GSM/GPRS technology and smartphone application " In: Proceedings of World Forum On Internet of things (WF-IoT), Seoul, IEEE world forum on internet
- 11- Mwesigwa (2013):" C An e-Health tele-media Application for Patient management. In: Proceedings of IST-Africa Conference and Exhibition (IST-Africa), Dublin, Ireland.
- 12- Nowicka, K. (2014):" Smart city logistics on cloud computing model.

Procedia Soc Behave Sic. [at:](#)

<https://www.researchgate.net/publication/277576118>

- 13- Rama, J.L. (2014) :” Legal Issues in Information Security "Jones & Bartlett Learning; two edition, PP 45-70.
- 14- Robert .M, Bernard .Racine , Robert .Michel (2001) : E-Strategy , Pure & Simple: Connecting Your Internet Strategy to Your Business Strategy Hardcover, McGraw-Hill, New York  
<https://www.amazon.com/Strategy-Pure-Simple-Connecting-Internet/dp/0071371788>
- 15- Roberto LA (2017):" Applications of Predictive Analytics in business intelligence" [https://www.neuraldesigner.com/blog/6 Applications of predictive analytics in business intelligence](https://www.neuraldesigner.com/blog/6_Applications_of_predictive_analytics_in_business_intelligence), Accessed 11 May.
- 16- Taylor, J. (2008): "Project Scheduling and Cost Control: Planning, Monitoring and Controlling the Baseline / Edition 1 "Publisher: Ross, J. Publishing, Incorporated, pp200-225.
- 17- Wrighton, Susanne & a Retie, Karl r (2016):" Cycle Logistics – moving Europe forward" The 9Th International Conference on City Logistics, Tenerife, Canary Islands (Spain), Pp950 – 958.
- 18- Ying, He, (2017): "Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organization " ".journal Informatics for Health and Social Care. volum 42: Pages 393-408  
<https://doi.org/10.1080/17538157.2016.1255629>