A Refereed Journal of Northern Europe Academy for Sudies & Research
--Denmark - 13/01/2020(Sixth issue)

The Role of Information Security Measures in Reducing the Risks of Information Security at Taif University

Prepare by

Dr. Adnan Al Shawabkeh

Taif University - Kingdom of Saudi Arabia

a_shawabkeh@yahoo.com

Abstract

This paper focuses on identifying the role of information security measures in reducing the risks of information security at Taif University. In order to achieve this aim, a questionnaire consisting of 52 items was designed to be distributed to the study sample of 129 employees. The study concluded that the security measures in reducing the risks of information security in the university are high. The security measures to prevent network hacking came at a high level, while security measures to prevent penetration through social engineering came at an average level. Also, malware security measures came at an average level. Information security measures helps in reducing internal, external, and natural risks to the system. The study recommended that the university administration classifies its information in a way that suits its work and maintain its data so as not to harm the system, improve the mechanisms of access control of the system, develop programs and procedures related to the administrative levels and authorities within the system, and focus on the security requirements of information, safety, and confidentiality.

Keywords: information security measures, network risk, social engineering risk, software security risk, information security

Introduction

IT crimes have become a serious phenomenon with negative effects in various fields, especially security, and the increase of their seriousness as a result of the development of information and communication technology is of significant importance. Therefore, measures must be taken to reduce the risks of information security in the organization. Information security represents the protection and security of all the resources of the organization and the preservation of the integrity and confidentiality of its information. Therefore, the organization's information must be maintained, protected, and damage should be minimized in regards to the risks the system may face.

To ensure the security of information in the organization, there are several ways to preserve it including the use of firewalls, passwords, and various methods of encryption. These methods prevent the disclosure of stored parameters that may affect the information assets of the organization.

Consequently, one of the ways to deal with the risks of information security in the organization is the physical element that provides physical protection of information systems; the technical component that supports and protects the security of information through the use of modern applications; and the human element that increases the efficiency and effectiveness of system personnel (Abdel Karim, 2013). In this study, the researcher attempts to identify the role of information security measures and their impact in reducing the risks of information security at Taif University.

The Study Problem

Due to the wide spread of IT applications, there has been a lot of risk of information security that threatens the information assets of the organization. This is because information has become vulnerable to theft, change, and unauthorized access. As a result of the importance of this information and the high value of many organizations, it is necessary to take appropriate measures to protect the sources of information from risks. Among these measures is "organized information security measures" which aim to verify the integrity of the organization and perform all its activities. Hence, the problem of the study can be shown in the following main question: What are the roles of information security measures in reducing the risks of information security at Taif University?

Study Questions

1. What are the information security procedures at Taif University?
2. What is the nature of internal information security risks?
3. What is the nature of external information security risks?
4. What is the nature of natural hazards?

Study Objectives

This study aims to achieve information security through the following:

1. To identify the most important information security measures put by the university on the information systems to reduce the risks to these systems.
2. Identify the most important internal threats to information systems at Taif University.
3. Identify the most important external threats that threaten information systems at Taif University.
4. Identify the most important natural hazards that threaten information systems at Taif University.

The Importance of the Study

This study is of significant importance because information systems are exposed to the risks that threaten the security and reliability of the data provided by these systems. The importance is due to the great development in information technology and the computer industry, which led to the easy copying, modification and change of data and files stored in computer memory. A similar development in the information security procedures was applied at the university. Therefore, the importance of the study includes:

1. Providing information security requirements at the university.
2. Maintaining the information system data at the university and developing ways to prevent its loss and maintain the future strategic plans of the university.
3. Protection of the security system of information at the university works to prevent the intrusion, modification or destruction of data.
4. Trying to link the role of information security measures and their impact in reducing the risks of information security.
5. Lack of studies that examine the risks to information systems in Saudi universities in general and at Taif University in particular.
6. Contributes positively to the development of security measures on information systems to reduce the risks of these systems.
7. To provide conclusions and recommendations that help to achieve the information security procedures at the university and maintain their confidentiality at various administrative levels through the preparation of awareness training programs for users.

Hypotheses of the Study

The First Main Hypothesis

Information security measures (prevention of intrusion through the computer network, social engineering and malware) contribute to reducing the risk of internal information security.

The Second Main Hypothesis

Information security measures (prevention of hacking through the computer network, social engineering and malware) contribute to reducing the risk of external information security.

The Third Main Hypothesis

Information security measures (prevention of intrusion through the computer network, social engineering and malware) contribute to reducing the risk of natural information security.

Theoretical Framework

Introduction

Information security measures are the starting point for the organization in all its operations. Therefore, it is considered an integrated process designed to prevent threats to the security of the organization and to provide safety measures to prevent intrusion of the hardware, software and computer network. It also ensures the provision of information security in the organization on computers and servers connected to the network, which might lead to data destruction (Abdul Karim, 2013).

The internal audit system creates a wide range of risk factors, including opportunities to steal assets of employees, the potential to lose operational information, and other risks and threats that cause business organizations to fail to achieve their objectives (Abdul-Jabbar, 2013).

Concept of Information Security Measures

This is a set of processes designed to achieve a set of objectives related to the reliability of operations in the organization and compliance with laws and regulations to control all processes within the organization and to reduce the risks to information security in the organization (Porter, et al., 2008).

Information Security Measures

Information security measures are important topics of concern to the management ahead of the significant importance of the strategy- which includes (Raval & Fichadia 2007):

1. The possibility of hacking systems, information or data, or modifying it, is not desirable, or it is modified before the user uses the system to talk to the target or not (Abdel-Jabbar, 2013).
2. Compliance with the requirements of protection and privacy laws, such as the specificity of information relating to employees, customers and suppliers (Abduljabbar, 2013).

Information Security

Information security is defined as the science that protects the information from the threats that threatens it or the barrier that prevents its attack by providing the necessary tools and means to protect it from internal or external risks. However, there are standards and procedures to prevent unauthorized access to information through communications, to ensure the authenticity and validity of such communications, and to protect against potential risks arising from the exploitation of vulnerabilities and weaknesses of the system (Raval & Fichadia, 2007).

The Importance of Information Security

The importance of information security stems from the fact that it is used by all users in the organization where there is a possibility of intrusion by users working in the organization. Therefore, the security of information is one of the most important issues that are discussed in the area of networks and security and confidentiality of information. This is as a result of the proliferation of viruses and spyware programs, the spread of the role of many IT specialists to deal with the organization to develop anti-virus programs and infiltration programs, and to focus on the level of interest in the implementation of procedures (Al-Salmi, 2001). The importance of information security stems from the following (Merkowand, 2005):

1. Procedures that prevent access to software with procedures that prevent the access or detection of the caller from entering the system.
2. Anti-virus equipment and software.
3. Constant change of passwords and encryption.
4. Rapid recovery plans in case of natural and environmental disasters.

Therefore, the development of an information security policy is one of the most difficult and sensitive issues. One of the priorities of IT management in the organization is to clarify it to users. The duties of each user and beneficiary of the information technology are known in advance (Raval & Fichadia, 2007). These are:

1. Accuracy of information and reliability of data extracted from the system.
2. Verifying user identity which includes the authentication of the identity of the persons authorized to access the system.
3. The accuracy and integrity of the security of operations and sources of the information system.
4. Reduce errors and risks in the system.
5. Protect the property of the Organization from damage, loss and misuse.
6. Increase the appropriateness and reliability of the information used for decision making.

Risks of Information Security

The risk and the distinction between the relevant concepts must be defined as follows:

1. **Threats :** This means the possibility of an organization being attacked by a person, such as a spy, hacker, intruder or anything threatening equipment or natural disasters (Anton, 2003).
2. **Risk :** This means the effect that occurs as a result of the threat action, that is, the event occurred as a result of a threat and the difference between the danger and the threat is that the

danger actually occurred, while the threat remains in the circle of probability (Schchter, 2004).

3. **Vulnerabilities :** Part of the system is likely to be achieved due to threat. This comprises of the port through which the threat is located after the danger. Generally, vulnerabilities are the drivers of threats and risk. There are two types of vulnerabilities:
    - **Technical Vulnerabilities:** It is the errors when designing the system, making it easy to make mistakes through them.
    - **Administrative Vulnerabilities:** These are weak administrative equipment and information storage places, which offer some risks (Marianne, 2009).

Classification of the Risks of Information Security

The risks of information security are classified according to different criteria, which includes the following:

1. Risks are classified into three categories: risks from the Internet, staff risks and natural hazards. They are classified into four sections: internal risks, external risks related to the Internet, physical risks and environmental risks (Noordegraff, 2002).
2. Classification of risks by objective (Bhoisi, 2011): - Risk can be classified here as deliberate risks and unintentional risks.

Sources of Security Risk

The literature on information security addressed many of the risks facing the information systems environment and was classified in terms of source (internal sources and external sources) (Warkentin & Willison, 2009) as follows:

Internal Sources

Internal sources occur because of one of the components of the system, which include the following:

1. **Human Risk:** This is the risk posed by individuals working in the system and is one of the most serious and most influential threats, and it includes intentional and unintentional acts by persons who are permitted and allowed to use the system (Goodhue & Straub, 2001).
2. **Equipment Malfunctions:** This is the breakdown of computer hardware, peripherals and network equipment associated with the system. This type of malfunction causes the system to stop working and to withhold service from the beneficiaries (Schechter, 2004).

3. **Software Errors:** Many of the software used in the system suffer from errors, which is reflected in the accuracy of the outputs and the correctness of the treatment performed by the system (Robert, 2010).
4. **Data Errors:** Errors resulting from the process of data entry. When an incorrect data is entered, it reflects in the accuracy of the output, and the greater the error in the data entered the greater the risk (Marianne, 2009).

External Risk

This type of risk is caused by factors outside the system. This can be as a result of persons who are not authorized to use the system. External risks also include environmental or natural causes. These risks include:

1. **Security Attack:** This means various attempts by unauthorized persons to gain illegal access to the system, or one of its components and risk factors (Heiser, 2013).
2. **Danger of Intrusion:** This means the arrival of persons who are not authorized to enter the system and carry out acts of sabotage such as data modification, theft or destruction (Kissel, 2013).
3. **e-baiting:** This means the attacker sends e-mail messages to deceive users such as fake electronic links similar to the website of the organization, or are fake electronic sites claiming to provide banking services. When the user accesses these sites, they ask him for his bank account information or credit card information. These sites are designed in a manner similar to real websites (Litan, 2004).
4. **Malware:** A small program designed to tamper with data, entered into the computer, without the user's knowledge to copy or remove the data recorded on it. Examples are computer viruses, worms, Trojans and time bombs (Merkowand James, 2005).

Natural or Environmental Risks

These risks are from the environment or the nature of the system, which is the risk of the system components such as hardware, software and the computer network. It includes fires, natural disasters, and power cuts (Hedi, 2006).

Threats Information

There are increasing threats to organizations that result in accelerated development of methods through which information can be accessed in an organization that is not designed to change its

target or destroy it. Information can be obtained in an unsolicited manner using various classification of thereat (Abdul-Jabbar, 2013) which are:

1. **Hacking:** The hacking process is through password cracking or hacking during an attempt to manipulate the zero-day-attack or Structured Query Language Injection Attack (Abduljabar, 2013).
2. **Social Engineering:** It aims to motivate the user to disclose the data of his research during the questions. This method can be done using several techniques as follows: (Abdul-Jabbar, 2013)
    - **Evil Twin:** It does not require the designated user to be aware of the contents of the specified file, which is required to use the file for its contents.
    - **Identity Theft:** If the recipient is identified as another user known to the user, it is required to provide the information directly.
    - **Phishing:** It is intended to access a virtual message from a destination (both known and unknown) to request or verify information. To achieve this, these messages are identified by a link in a known destination.
3. **Malware:** This is the process of intrusion through a specialized program to facilitate the infiltration of the system and the network to destroy the data. The installation of the program is difficult to remove, and it contains this method on several techniques using the following (Abdul-Jabbar, 2013):
    - **Trojan Horse:** This is a program that claims to rid your computer of viruses, but it instead introduces viruses into your computer.
    - **Viruses:** These are programs that access the files stored in the computer and causes the destruction of these files.
    - **Spyware:** These are software that causes personal information to be accessed without the knowledge of the user. It is a form of malware that hides on your computer, monitors your activity, and steals sensitive information like bank details and passwords.

Previous Studies

This study aimed to clarify the role of IT governance in reducing these risks so as to reduce electronic financial manipulation in light of the application of government units to e-government system in theory. The study reached a number of results. Thus, the most important of which are:

1. The application of the e-government system faces some difficulties and risks that threatens the security of government information and makes it vulnerable to loss of confidence of its clients and beneficiaries in it. Thus, the most important of which is electronic financial manipulation.
2. IT governance mechanisms contribute to achieving information security requirements and reducing the risks to which they are exposed.

The study recommended the development of the procedures of the internal control system in reducing electronic financial manipulation.

The Study of Al-Danf (2013)

This study aimed at understanding the reality of the information systems security administration in the technical colleges in the Gaza Strip. The researcher used a descriptive analytical research methodology. The study society consisted of the employees of the information systems in the technical colleges. The study tools used for data collection were questionnaire and the interview. Based on a set of results, the most important of which were:

1. Information systems infrastructure is available in technical colleges at a medium level.
2. Higher departments of technical colleges are aware of the importance of information security policies, but none of the colleges have policies in place which are applied on a clear basis.
3. Technical colleges vary in the society of the study in degrees of use of their information systems.
4. There are statistically significant differences in the views of the study sample on the reality of the security management of information systems in technical colleges.

The study recommended the establishment of "information security policies for their information systems, and their dissemination, application, development, review and risk assessment on a regular basis to find out ways to restore work and develop contingency plans to ensure the security of information systems."

In the study, a questionnaire was designed for this purpose. 48 questionnaires were distributed: 43 of which were to Islamic banks and the others to about 3 banks. The study reached a number of results, and the most important of which were:

1. The effectiveness of the control system to study the risks that threaten the security of information in the system.

2. The effectiveness of the procedures of the internal control system and its ability to detect errors, fraud and manipulation.

The study recommended that internal control studies the risks resulting from the application of computerized information systems and the risks resulting from the employees, as well as the need to protect the assets, files, and devices from misuse and impose penalties by the administration when any violations emerges due to the lack of trust.

Furthermore, this study aimed to explore the state of information security and to work towards a better understanding of the prevailing facts in this field within Saudi Arabia. The study used the survey method. A pre-selection of a group of 280 Saudi organizations are represents shareholders from four major sectors. The researchers organized a workshop for the representatives of these different organizations. The researchers also prepared a questionnaire that was distributed to the participants and the response rate was 75.5%. The study reached a number of results, and the most important of which were:

1. The importance of information security policy in ensuring the adoption of appropriate control factors. The study showed that more than half of the organizations have an information security policy. Majority of them tend to apply it while 89% periodically review this policy.
2. Consider Access Control as critical to information security.
3. Addressing information security issues distinguishing between information sensitivity.

Therefore, the study recommended the importance of establishing security awareness within institutions through specialized knowledge training. The study used the descriptive method and the questionnaire as a tool for study. The study community was composed of all employees of the websites. A sample was collected at random and was stratified consisting of 195, 111, which were distributed to the security services, and 84 to the civilian bodies. The study reached a number of results, and the most important of which are:

1. The extent to which information security measures and the organization of information security in the civil and security websites are compatible with security and civil security standards.
2. Information security technologies, the information security environment, and the information security of the human element in the websites of the two sectors are consistent with international and local standards.

The study recommended the need for government agencies to implement a significant part of the international standard for information security as well as the unification of the authorities responsible for the implementation and follow-up of government information security through a government-run agency.

Furthermore, the study was designed to identify these risks and to achieve the objectives of the study. The descriptive and inductive analysis method was used by collecting information from Arabic and foreign books, periodicals and articles, in addition to the field study based on the distribution of the questionnaire. The sample consisted of 85 questionnaires distributed to 16 Jordanian banks with 5 responses from each bank. The response rate was 92% and the security risks of the electronic accounting information systems were based on the validity and credibility of the financial statements of the Jordanian commercial banks. Therefore, the study reached the following results:

1. Commercial banks are exposed to several risks to the security of their electronic accounting information systems.
2. The security measures put in place by Jordanian commercial banks limit the risks of electronic accounting information security.

The study recommended the need for commercial banks to monitor the extent to which the controls applied by them are applied to limit the risks to which the bank is exposed, and to evaluate the appropriate procedures to limit the risks of information security.

The Study of Zuhairi (2015)

The study aimed to identify the risks faced by information systems and the main reasons for their occurrence and strategies in addressing them. Here, a questionnaire was distributed to all employees in the Syrian banks located in the Syrian coast. The study reached the following results:

1. There are measures to address the risks facing information systems.
2. No risk of electronic accounting information systems occur frequently in Syrian banks.
3. There are adequate safeguards to address the security risks of electronic accounting information systems.

Therefore, the study recommended that the accuracy of data entry by employees and lack of disclosure of passwords should be checked.

The Study of Al Hanini (2012)

This study aims at raising the level of information systems in the Jordanian banking system. To achieve this, a questionnaire was formed and distributed to the study sample. This consists of 63 participants who are assistants to the general managers, the director of departments, the managers and their assistants, and the employees of the Jordanian banks. After the analysis of the data using the SPSS program, the study reached the following results:

1. One of the most important risks faced by the bank is that there is no experience for employees to maintain information security.
2. Risks that threaten information systems in banks regarding data entry by employees.
3. There are internal risks that threaten the system, including the misinterpretation of data.
4. There are external risks that threaten the system, including viruses.
5. There are natural and abnormal hazards faced by employees.

The study recommended that the bank should put in place control measures to reduce the effects of systems risks and update the means of protection according to technological development and to hold courses for employees and train them on these procedures.

This study aimed to identify the role of the human element in the field of information systems security and it focuses on the factors that affect the security behavior of employees and how they look at the security measures against internal threats. The qualitative approach was used, and its tools were the interviews on users of information security. It also entails the review and analysis of documents, and the direct observation of the behavior of users. The study reached the following results:

1. Satisfaction and acceptance of employees and security measures are important elements in achieving security behavior towards the security of information systems.
2. Staff experiences difficulty and complexity in understanding documents related to information security.
3. The application of human requirements for information security needs to be aware of the importance of information security.

Therefore, the study recommended that an assessment should be made in regards to the actions of employees towards various security issues to improve information security. In addition, they should be informed of the advantages in the application of countermeasures to reduce the risks to which information systems are exposed in the organization.

Methodology of the Study

In order to achieve the objectives of the study, the descriptive and field curriculum was used. The previous studies and theoretical research in the area of information security were reviewed in order to clarify the concept of information security measures, the risks of information security (internal and external sources), and the threats to the information security in the organization. From the sample of the faculty members at the university, the study tool was evaluated and the paragraphs were modified if there was an amendment. Also, the data collected through the questionnaires distributed to the sample of the study were analyzed using appropriate statistical methods such as Statistical Program for Social Sciences (SPSS). After analyzing the data and testing the hypotheses of the study, the results were drawn.

The Study Community

The current study community includes the employees of the university administration who use the system and deal with it daily, both administrative and technical. This is in addition to IT staff in the Deanship of Information Technology and Technical Support and the Faculty of related computers. Out of total of 160 questionnaires distributed, 138 were retrieved. Nine questionnaires were excluded due to lack of seriousness when filled. Thus, the number of questionnaires valid for statistical analysis was 129 (80.6%).

Characteristics of Study Sample Individuals

The following table shows the distribution of the sample of the study according to personal and functional variables.

Table 1. Frequency and percentage according to personal and functional variables (age, job role, qualification, grade, job experience and training courses in the field of information technology)

Variable	Category	frequency	percentage %
Age	Less than 30 Year	19	14.7 %
	31 – 40 Year	49	38 %
	41 – 50 Year	34	26.4 %
	51 Year and Above	27	20.9 %
	Total	129	100 %
Qualification	Diploma/intermediate or below	9	6.8 %
	Bachelor's Degree	78	60.6 %
	Master Degree/Higher Diploma	23	17.9 %
	PhD	19	14.7 %
	Total	129	100 %

Job role	Administrative	23	17.8 %
	Financial	32	24.8 %
	Information Technology	53	41.1 %
	Information System	21	16.3 %
	Total	129	100 %
Grade	Manager	9	6.8 %
	Head of Department (HOD)	18	13.9%
	Principal Officer	73	56.7 %
	Junior Officer	29	22.6 %
	Total	129	100 %
Job experience	Less Than 5 Years	13	10.1 %
	6 – 10 Years	25	19.4 %
	11 – 15 Year	33	25.6 %
	16 years and above	58	44.9 %
	Total	129	100 %
IT training courses	None	18	13.9 %
	1 – 5 courses	29	22.6 %
	6 – 10 courses	39	30.2 %
	Above 11 courses	43	33.3 %
	Total	129	100 %

The results in Table 1 show that the characteristics of the individuals in the research sample are close to all personal and functional characteristics. The majority of the age group (31-40 years) was 38%. This percentage is qualified in the field of information technology and specializes on the means of protection for information security. Also, it deals with it well and reduces the risks to the system, where 41.1% are the employees who serve as executive staff (Principal Officer). 56.7% of the study sample had a job experience between 11-15 years with 44.9% of those undergoing specialized more than 11 training courses in the field of Information Technology.

Study Tool

The questionnaire was used in the collection of data. The questionnaire consisted of three parts as follows:

1. The first part includes the personal and functional characteristics of the sample of the study.
2. The second part consists of three dimensions:
    - The first dimension is to prevent hacking through network attempts.
    - Second Dimension: Prevention of Penetration through Social Engineering.

- Third Dimension: Prevention of Malware Infection (Trojans and Viruses).

3. Information Security Risks (Internal, External and Natural).

Validation of the Study Tool and its Stability

In order to ensure that the questionnaires actually measure the study variables that were determined to be measured during the construction stages of the questionnaire, they were presented to a number of arbitrators for their opinion. This is in addition to the distribution of the questionnaire to a sample of 20 faculty members to identify the clarity and ease of words used and their understanding of the concepts contained in this questionnaire and then make the necessary adjustments.

The coefficient of consistency was used to determine the compatibility of the measuring instrument and the computer-processed results as shown in Table 2. The results show that the stability coefficient for all dimensions is not less than 60%. The stability coefficient for all the paragraphs of the questionnaire was 83.8%. This means that the study instrument is stable and valid for statistical analysis and scientific research (Sekaran, 2006).

Table 2. Results of Alpha-Cronbach Alpha (α) for the study variables

Variables	Dimensions	No. of items	Stability Coefficient Cronbach – Alpha (α)
Independent variables (With its three dimension)	**Information security measures**		
	Hacking through the computer network	*6*	*83.2 %*
	Hacking through social engineering	*6*	*76.5 %*
	Hacking through malware	*6*	*85.3 %*
The dependent variables (With its three dimension)	**Information security risks**		
	Internal risk	*16*	*90.9 %*
	External risk	*10*	*81.6 %*
	Natural risk	*7*	*85.3 %*
Total		***52***	***83.8 % %***

Study Variables and Definitions of Terms

The Independent Variable

Information Security Measures

This measure ensures the protection of information from the threats that threatens them, and the prevention of aggression by providing tools and means to protect information from internal, external or natural risks because of gaps or threaten or threaten The system (Abdul-Jabbar, 2013), including the following:

- **Hacking:** Accessing information through the computer network to modify, destroy or steal data and information (Romney & Steinhart, 2012).
- **Social Engineering:** The computer helps to clarify some of their own confidential information through simple questions with a view of retrieving information (Romney & Steinbart, 2012).
- **Malware:** Process of penetration through specialized programs to access the network, such as Trojan Horses and Viruses (Romney & Steinhart, 2012).

The Dependent Variable

Information Security Risks

These are weaknesses or gaps in a security program that can be exploited by threats as a result of an illegal access from internal, external or natural sources (Al-Buhaisi, 2011). They are described as follows:

Internal Risks: These risks are caused by authorized persons, and it performs a work that violates the security of the data and the risk of internal penetration. This security threat occurs due to lack of knowledge on the parts of the system users, which result to the loss of data.

External Risks: These risks are caused by unauthorized persons, and it performs a work that violates the security of the data and the risk of external penetration. The unauthorized person, such as hackers, gains access to the system by exploiting the gaps in it and uses malicious programs such as computer viruses gain access to the system and its components. An electronic hijacker is someone that breaches the security of a system by sending malicious emails with the intention of vandalism, password theft, or spyware.

Natural Hazards: These are risks to which the system is naturally exposed to, such as natural disasters, power failures, technical malfunctions in the physical equipment, software and computer network, causing a violation of the security system either by slow processing or a stop in the work process.

Statistical Analysis

The Statistical Package for Social Sciences (SPSS) programs was used in the analysis of the data. The descriptive statistics were used, while the Alpha (α) coefficient was designed to ensure the stability of the resolution clauses. The multiple regression analysis tested the effect of each

independent variable and its dimensions on the variable (F) to verify the significance of the relationship between the variables of the study.

Results of Statistical Analysis

The various statistical methods were used to test the sample of the study and its hypotheses. The five-dimensional Likert scale was used in the study.

Based on the values of the arithmetic averages, the data will be interpreted as follows for the intervals between 1.00 - 2.33. This indicates that the level of perceptions of the members of the study sample is low. If the mean of the arithmetic mean is between 2.34 - 3.66, the level of perception of the members of the study sample are average. Finally, if the mean of the arithmetic average is between 3.67 - 5.00, it indicates that the level of perception of the members of the study sample is high. The results of the statistical analysis were as follows:

The Independent Variable: Information security procedures were divided into two axes and three dimensions as follows:

First : The sample of the study of information security measures to prevent hacking was measured through Paragraphs 1 – 7 :

1. To sensitize users about the information security policies implemented throughout the university.
2. The security system provides a mechanism to verify the identity of the entrants to the system and the network, even when they access it through their mobile phones, and register their actions.
3. Determine the powers of the users of each system.
4. There is no system log file.
5. There are access restrictions to the system and the information network of the authorized persons.
6. The system is checked and verified.
7. Software is used to help increase network access settings such as Firewall and Proxy.

Table 3. The arithmetic mean, the standard deviation, the calculated t value, and the degree of perception of the sample members

Paragraph No	Mean	Standard Deviation	Calculated t value	Degree of Perception	Ranking	Frequency				
						1	2	3	4	5
1	3.62	1.019	6.65	Average	5	25	0	28	50	26

2	**3.77**	**1.163**	**7.49**	**High**	**1**	**26**	**2**	**26**	**26**	**49**
3	**3.72**	**1.142**	**7.02**	**High**	**3**	**27**	**0**	**27**	**32**	**43**
4	**3.73**	**1.210**	**6.84**	**High**	**2**	**26**	**0**	**27**	**27**	**49**
5	**3.72**	**1.135**	**7.06**	**High**	**4**	**25**	**1**	**26**	**36**	**41**
6	**3.61**	**1.162**	**5.91**	**Average**	**6**	**26**	**3**	**26**	**38**	**36**
7	**3.60**	**1.155**	**5.94**	**Average**	**7**	**25**	**3**	**28**	**37**	**36**
High	**3.67**	**0.329**	**23.19**	**High**						

Table 3 shows that the general average of the sample of the study of the security measures to prevent hacking through network hacking (theft of the words of the treatment of intrusion vulnerability during previous processing attempts and database injection attacks) was high. Thus, the mean was 3.67 and the standard deviation was 0.329. Paragraph 2 "System provides a mechanism to verify the identity of the entrants to the system and the network, even when they access it through their mobile phones, and register their actions" shows the highest mean of 3.77 and a standard deviation of 1.163. In order to verify the accuracy of the assessment of the individuals of the research sample, the t-test and the associated significance were used. It was found that the calculated t value of 23.19 and its significance level (0.000) is statistically significant, indicating the significance of the estimate based on the arithmetic mean.

Second : Evaluation of the sample members of the study of information security measures to prevent penetration through social engineering were measured in paragraphs 8 – 13 :

8. The request was made directly by a relative or colleague or friend about the information entering the system.
9. Right to access information on the system in places easy to detect by others.
10. Was blackmailed by a certain person by providing access to the information on the system.
11. You receive messages containing attachments from an anonymous source.
12. The messages you receive contain a fake link to a known destination.
13. Expose your device to illegal and unauthorized access.

Table 4. The arithmetic mean, the standard deviation, the calculated t value, and the degree of perception of the sample members

Paragraph No	**Mean**	**Standard Deviation**	**Calculated t value**	**Degree of Perception**	**Ranking**	**Frequency**				
						1	**2**	**3**	**4**	**5**
8	***3.72***	***1.104***	***7.42***	High	**1**	**25**	**0**	**26**	**38**	**40**

9	***3.56***	***1.205***	***5.26***	Average	**6**	**26**	**5**	**26**	**36**	**36**
10	***3.67***	***1.113***	***6.80***	High	**2**	**25**	**1**	**27**	**39**	**37**
11	***3.65***	***1.164***	***6.36***	Average	**4**	**26**	**2**	**26**	**37**	**38**
12	***3.58***	***1.164***	***5.67***	Average	**5**	**26**	**3**	**29**	**35**	**36**
13	***3.65***	***1.130***	***6.55***	Average	**3**	**26**	**1**	**28**	**36**	**38**
Average	**3.64**	***0.524***	**13.84**	**Average**						

Table 4 shows that the general mean for the assessment of the members of the study sample for information security measures to prevent penetration through social engineering was average. The mean was 3.64 and the standard deviation was 0.524. Paragraph 8 achieved the highest mean of 3.72 and with a standard deviation of 1.104. In order to verify the accuracy of the assessment of the individuals of the research sample, the t-test was used and its significance level. Here, it was found that the general value of t calculated is 13.84 and its significance level (0.000) is statistically significant at $\alpha \leq 0.05$.

Third : Evaluation of the sample members of the study of information security measures to prevent penetration through malware (Trojans and viruses) was measured through paragraphs 14 – 19 :

14. There is strict censorship that prevents the download of files from the Internet.
15. There is a secret software that prevents the penetration of computer user information without his knowledge.
16. Software update periodically and continuously.
17. Uses software that resists viruses and is constantly updated.
18. Use modern and sophisticated software to protect the system from hacking.
19. There are restrictions in the use of UBS and CD-ROM.

Table 5. The arithmetic average, the standard deviation, the calculated t value, and the degree of perception of the sample members

Paragraph No	**Mean**	**Standard Deviation**	**Calculated t value**	**Degree of Perception**	**Ranking**	**Frequency**				
						1	**2**	**3**	**4**	**5**
14	**3.69**	**1.110**	**7.06**	High	**1**	**26**	**0**	**27**	**37**	**39**
15	**3.65**	**1.101**	**6.71**	Average	**2**	**26**	**5**	**30**	**36**	**37**
16	**3.60**	**1.156**	**5.87**	Average	**5**	**25**	**3**	**29**	**36**	**36**
17	**3.58**	**1.102**	**5.99**	Average	**6**	**25**	**2**	**29**	**42**	**31**
18	**3.63**	**1.104**	**6.46**	Average	**4**	**26**	**1**	**27**	**41**	**34**

19	**3.64**	**1.117**	**6.54**	Average	**3**	**26**	**1**	**27**	**39**	**36**
Average	**3.63**	**0.612**	**11.73**	Average						

Table 5 shows that the general average for the assessment of the members of the study sample of the information security measures through the use of malware (Trojans and viruses) was high. The mean was 3.63 and the standard deviation was 0.612. Paragraph 14 "There is strict censorship that prevents the download of files from the Internet" achieved the highest mean of 3.69 with a standard deviation of 1.110. In order to verify the accuracy of the assessment of the individuals of the research sample, the t-test and its associated significance were used. It was found that the calculated value of t is 11.73 and its significance level is 0.000, which is statistically significant, indicating the significance of the estimate based on the arithmetic mean.

Dependent Variable

Information security risk is divided into three dimensions, as follows:

First: Internal risks to which information security is exposed and measured through paragraphs 20 – 35 :

20. The system was hacked by a user of the system causing the system to stop working for a while.
21. The system was hacked by a user of the system causing the system to slow down.
22. The system was hacked by a user of the system causing incorrect output.
23. The system was hacked by a user of the system causing the data to be stored.
24. Deliberately inserting the data into the system resulted in incorrect output.
25. The unintentional input of the data into the system caused the system to stop functioning for a while.
26. The unintentional input of the data into the system led to incorrect output.
27. Improper unintentional input of data provides incorrect output.
28. Improper misuse of the system causes the system to stop functioning for some time.
29. The deliberate misuse of the system causes the destruction of stored data.
30. Unintentional damage to system equipment causes the system to stop functioning for some time.
31. The unintended destruction of system equipment causes the destruction of stored data.
32. Errors in the system design led to slow system operation.
33. Errors in the system design resulted in incorrect output.

34. Errors in the system design caused the system to stop working for a period.
35. Errors in the system design led to the destruction of stored data.

Table 6. The arithmetic mean, the standard deviation, the calculated t value, and the degree of perception of the sample members

Risk paragraphs	Paragraph No	Mean	Std. Dev.	Calc.t value	Degree of perception	Frequency				
						1	2	3	4	5
Internal penetration	20	*3.11*	*1.38*	*0.89*	Average	26	21	26	30	26
	21	*3.15*	*1.38*	*1.21*	Average	26	20	26	29	28
	22	*3.09*	*1.37*	*0.78*	Average	26	21	27	30	25
	23	*3.11*	*1.38*	*0.89*	Average	26	21	26	30	26
General	20 - 23	*3.12*	*1.36*	*0.94*						
Intentional misinterpretation	24	*3.23*	*1.34*	*1.97*	Average	25	17	26	33	28
General	24	*3.23*	*1.34*	*1.97*	Average					
Unintentional wrong input	25	*3.22*	*1.34*	*1.85*	Average	25	17	27	33	27
	26	*3.20*	*1.34*	*1.71*	Average	26	17	27	32	27
General	25 -26	*3.21*	*1.35*	*1.78*	Average					
Improper misuse	27	*1.69*	*1.35*	*3.20*	Average	25	18	26	33	27
	28	*1.56*	*1.35*	*3.19*	Average	26	18	26	32	27
	29	*1.43*	*1.35*	*3.17*	Average	27	18	26	31	27
General	27 - 29	*1.45*	*1.35*	*3.19*						
Int. change of sys. equipment	30	*3.18*	*1.35*	*1.45*	Average	*27*	*31*	*27*	*18*	*26*
	31	*3.19*	*1.33*	*1.59*	Average	*27*	*30*	*29*	*17*	*26*
General	30 - 31	*3.19*	*1.34*	*1.55*						
Program errors	32	3.26	1.37	2.13	Average	25	17	26	30	31
	33	3.23	1.35	1.96	Average	25	17	27	31	29
	34	3.21	1.34	1.78	Average	27	16	29	28	29
	35	3.21	1.34	1.78	Average	26	17	27	33	27
General	32 - 35	3.23	1.32	1.91	Average					
Total of Internal risk as a whole		3.18	0.878	2.38	Average					

Table 6 shows the mean, standard deviation, level of perception, and frequency for the internal risk assessment of the sample and the measures measured by the sample. The majority of the answers to the sample were "approved", which limits the risk of information security due to unintentional misuse and unintentional damage. On the other hand, the risk of inadvertent misinformation and program errors are less likely to occur. This meant that internal risks were within the acceptable level and that the safeguards were appropriate, but more control was required by the system administrator Information security measures, as well as verification of the integrity of the code from time to time.

Second: External risks to the security of information were measured through paragraphs 36 – 45:

36. The system was hacked by hackers causing the system to stop working.
37. The system was hacked by hackers causing slow system action.
38. The system was hacked by hackers causing incorrect output.
39. The system was hacked by hackers causing the data to be destroyed.
40. The system has stopped working for a while because it was attacked by malicious programs (viruses and the like).
41. The system was attacked by malicious programs (viruses and similar) causing slow system action.
42. The system was attacked by malicious programs (viruses), causing the inability to obtain the appropriate output for the decision maker.
43. The system is exposed to attack by malicious programs (viruses and similar) causing the destruction of stored data.
44. The system was attacked by emails causing the system to stop working for a while.
45. The system was attacked by e-mails causing the data to be destroyed.

Table 7. The arithmetic mean, the standard deviation, the calculated t value, and the degree of perception of the sample members

Risk paragraphs	Paragraph No	Mean	Std. Dev.	Calc.t value	Degree of perception	Frequency				
						1	2	3	4	5
External penetration	36	3.22	1.35	1.83	Average	26	17	26	32	28
	37	3.24	1.37	1.99	Average	26	17	26	29	31
	38	3.22	1.35	1.82	Average	26	17	27	30	29
	39	3.26	1.36	2.21	Average	26	16	26	30	31
General	36-39	3.24	1.36	1.96	Average					
Malicious Software	40	3.25	1.36	2.08	Average	*25*	*17*	26	*31*	*30*
	41	3.26	1.36	2.21	Average	*26*	*16*	26	*30*	*31*
	42	3.25	1.36	2.08	Average	*27*	*16*	26	*29*	*31*
	43	3.19	1.39	1.58	Average	*26*	*19*	26	*27*	*31*
General	40-43	3.24	1.37	1.99	Average					
Elect. Phishing	44	3.21	1.37	1.73	Average	26	18	26	29	30
	45	3.26	1.35	2.16	Average	26	16	26	31	30
General	44 - 45	3.24	1.36	1.95	Average					
Total External risk as a whole		3.26	1.348	2.16	Average					

Table 7 shows the mean, standard deviation, degree of perception, and frequency for the external risk assessment of the sample and the measures measured by the sample. The majority of the answers to the sample were "strongly approved and approved", which limits the risk of

information security due to unintentional misuse and software errors. On the other hand, the risk of inadvertent misinterpretation was less likely to occur. This meant that internal risks were within the acceptable level and that the safeguards were fairly appropriate, but more control was required by the system administrator Information security measures, as well as verification of the integrity of the code from time to time.

Third: The natural hazards to which information security is exposed and measured through paragraphs 46 - 52 :

46. Loss of data due to natural disasters.
47. The system is temporarily suspended due to natural disasters.
48. Data loss due to sudden power outages.
49. The system is stopped for a period due to power outage for a reason outside the Directorate.
50. The system is stopped for some time due to technical faults that occurs in the system normally.
51. Obtain incorrect output from the system due to technical faults.
52. Loss of data due to technical failures occurring in the system.

Table 8. The arithmetic mean, the standard deviation, the calculated t value, and the degree of perception of the sample members

Risk paragraphs	Paragraph No	Mean	Std. Dev.	Calc.t value	Degree of perception	Frequency				
						1	2	3	4	5
Natural Disaster	**46**	***3.19***	***1.36***	***1.64***	Average	**26**	**18**	**27**	**29**	**29**
	47	***3.28***	***1.35***	***2.34***	Average	**25**	**16**	**26**	**31**	**31**
General	**46 - 47**	***3.24***	***1.36***	***1.99***	Average					
Blackouts	**48**	***3.24***	***1.35***	***2.02***	Average	***25***	***17***	***26***	***32***	***29***
	49	***3.28***	***1.35***	***3.34***	Average	***25***	***16***	***26***	***31***	***31***
General	**48 - 49**	***3.26***	***1.35***	***2.18***						
Technical Fault	**50**	***3.22***	***1.37***	***1.86***	Average	***27***	***17***	***26***	***28***	***31***
	51	***3.20***	***1.37***	***1.68***	Average	***26***	***18***	***26***	***30***	***29***
	52	***3.23***	***1.36***	***1.94***	Average	***26***	***17***	***26***	***30***	***30***
General	**50 - 52**	***3.15***	***1.37***	***1.83***	Average					
Total of Natural risk as a whole		***3.23***	***0.86***	***3.10***	Average					

Table 8 shows the mean, standard deviation, degree of perception, and frequency of the sample's estimate of natural hazards and the items measured by them. It was average. Most of the responses to the sample were "strongly approved and approved" due to unintentional misuse and program errors. On the other hand, the risk of inadvertent misinterpretation was the least of these risks. This means that internal risks are within the acceptable level and that the safeguards are

fairly appropriate, but more supervision is required by the system administrator Information security measures, as well as verifying the integrity of the code from time to time.

Hypotheses Testing

The First Main Hypothesis

Information security measures (intrusion prevention through the computer network, social engineering and malware) contribute to reducing the risk of internal information security.

Table 9. Simple regression analysis of the impact of information security measures in reducing the risks of internal information security

Dependent Variable	R	R^2	Calculated F value	D f Degree of Freedom		Sig.*	Decision
Risk of internal information security	0.661[a]	0.437	32.386	Regression	3	0.000[b]	Accept the Hypothesis
				Residual	125		
				Total	128		

a. Predictors: (Constant) : - Prevent intrusion through the computer network, social engineering and malware

* The correlation is statistically significant at ($\alpha \leq 0.05$)

Explanatory Power of the Model

The results of the statistical analysis showed a statistically significant effect of the dimensions of the independent variable (preventing penetration through the computer network, social engineering and malware) in reducing the risks of internal information security. The coefficient of correlation was R = 0.661 at ($\alpha \leq 0.05$) and R^2 = 0.437. The independent variable was able to explain 43.7% of the change in internal information security risk, while the rest is due to other factors including random error. The value of sig (0.000) and the model is valid for testing. Therefore, Table 10 shows the values of T, β values, and sig values.

Table 10. The impact of information security measures in reducing the risks of internal information security

Model	Standardized Coefficients	t	Sig.
	Beta β		
Constant	1.047	1.312	0.192
Preventing intrusion through the computer network	0.113	2.071	0.049
Prevent penetration through social engineering	0.515	3.938	0.000
Prevent hacking through malware	0.663	5.954	0.000

a. Dependent Variable: - Risks of internal information security

Morality of the Model

In order to determine the significance of the regression coefficients, we will use the P Value of the T statistic. It was found that all the dimensions of the independent variable have a significant effect after the dependent variable. The internal information security risk based on the value of T and its significance level is statistically significant at $\alpha \leq 0.05$. The impact of the procedures to prevent penetration through malware ($\beta = 0.663$) is followed by the prevention of penetration through social engineering with the value of the effect $\beta = 0.515$, and is also followed by the prevention of hacking through the computer network where the value of the effect $\beta = 0.113$. This shows that attention to information security limits the security risks for internal information (66.3%, 51.5% and 11.3% respectively).

The values of sig. is given as 0.000, 0.000, and 0.049 respectively. The significance of this effect is the calculated F value of 32.386 which is a statistical function at $\alpha \leq 0.05$, which confirms the validity of the first hypothesis.

The Second Main Hypothesis

Information security measures (prevention of hacking through the computer network, social engineering and malware) contribute to reducing the risk of external information security.

Table 11. Simple regression analysis of the impact of information security measures in reducing the risk of external information security

Dependent Variable	R	R^2	Calculated F value	D f Degree of Freedom		Sig.*	Decision
Risk of external information security	0.596[a]	0.355	22.934	Regression	3	0.000[b]	Accept the Hypothesis
				Residual	125		
				Total	128		

a. Predictors: (Constant) : - Prevent intrusion through the computer network, social engineering and malware

* The correlation is statistically significant at ($\alpha \leq 0.05$)

Explanatory Power of the Model

The results of the statistical analysis showed a statistically significant effect of the dimensions of the independent variable (preventing penetration through the computer network, social engineering and malware) in reducing the risk of external information security. The coefficient of correlation R = 0.596 at the level of significance ($\alpha \leq 0.05$) and the coefficient of determination $R^2 = 0.355$ means that the dimensions of the independent variable could explain 35.5% of the

change in the risk of external information security and the rest due to other factors, including random error. The value of sig (0.000) and the model is valid for testing. Table 12 shows the values of T, β values, and sig values.

Table 12. The impact of information security measures in reducing the risks of external information security

Model	Standardized Coefficients Beta β	t	Sig.
Constant	0.425	0.565	0.573
Preventing intrusion through the computer network	0.349	2.279	0.038
Prevent penetration through social engineering	0.549	4.464	0.000
Prevent hacking through malware	0.408	3.897	0.000

a. Dependent Variable: - Risks of external information security

Morality of the Model

To determine the significance of the regression coefficients, we will use the P value of the T statistic. All the dimensions of the independent variable have a significant effect on the dimension of the dependent variable. The external information security risk is based on the value of T, which is statistically significant at $\alpha \leq 0.05$. Breakthrough by social engineering $\beta = 0.549$ followed by procedures to prevent penetration through malicious software with the value of the effect of $\beta = 0.408$ followed by the prevention of hacking through the computer network where the impact value $\beta = 0.349$, shows that attention to information security measures reduce the risk of information security (54.9%, 40.8%, and 34.9% respectively).

The values of sig. is given as 0.000, 0.000, and 0.038. The significance of this effect is the calculated F value of 22.934 which is a statistical function at $\alpha \leq 0.05$, which confirms the validity of the second main hypothesis.

The Third Main Hypothesis

Information security measures (intrusion prevention through the computer network, social engineering and malware) contribute to reducing the risks of natural information security.

Table 13. Analysis of the simple regression of the impact of information security measures in reducing the risks of security of natural information

Dependent Variable	R	R^2	Calculated F value	D f Degree of Freedom		Sig.*	Decision
Risk of natural information security	0639[a]	0.408	28.697	Regression	3	0.000[b]	Accept the Hypothesis
				Residual	125		

				Total	128		

a. Predictors: (Constant) : - Prevent intrusion through the computer network, social engineering and malware

* The correlation is statistically significant at ($\alpha \leq 0.05$)

Explanatory Power of the Model

The results of the statistical analysis showed a statistically significant effect of the dimensions of the independent variable (prevention of penetration through the computer network, social engineering and malware) in reducing the risks of the security of natural information. The coefficient of correlation was R = 0.639 at $\alpha \leq 0.05$, and $R^2 = 0.408$, i.e. the dimensions of the independent variable were able to explain 40.8% of the change in the risks of the security of natural information and the rest due to other factors including random error. The value of sig (0.000) and the model is valid for testing.

Table 14 shows the values of T, β values and sig values.

Table 14. The impact of information security measures in reducing the risks of internal information security

Model	Standardized Coefficients	t	Sig.
	Beta β		
Constant	1.185	1.473	0.143
Preventing intrusion through the computer network	0.491	2.488	0.026
Prevent penetration through social engineering	0.519	3.938	0.000
Prevent hacking through malware	0.605	5.392	0.000

a. Dependent Variable: - Risks of natural information security

Morality of the Model

To determine the significance of the regression coefficients, we will use the P value of the T statistic. All the dimensions of the independent variable are significantly affected after the dependent variable. The risk of the security of natural information is based on the value of T, which is statistically significant at the level ($\alpha \leq 0.05$). The penetration rate through malware was β = 0.605, followed by the prevention of penetration by social engineering. The value of the effect was β = 0.519 followed by the procedures of preventing penetration through the computer network where the impact value is β = 0.491. Thus, this means that attention to information security measures limits the risk of information security Interior (60.5%, 51.9%, and 49.1%, respectively).

The values of sig. is given as 0.000, 0.000, and 0.026. The calculated value of F, which was 28.697, was statistically significant at $\alpha \leq 0.05$, which confirms the validity of the third main hypothesis.

Results

The study showed the following results:

1. The security measures that help in reducing the security risks that would occur on the information system at the university were high.
2. The security measures to prevent hacking through network Hacking came at a high level with an average of 3.67.
3. The security measures to prevent penetration through social engineering came at an average level of 3.64.
4. The security measures to prevent malware hacking came at an average level of 3.63.
5. The accuracy of the evaluation of the sample of the study sample was verified, using t-test and its significance was statistically significant, indicating the significance of the estimate.
6. Information security measures contribute to the reduction of internal, external and natural risks to the system.

Recommendations

The study recommends the following:

1. The university administration should classify its information in a way that suits its work and maintain its data in such a way to ensure that the system is not harmed.
2. Improve the mechanisms of access control of the system and the development of programs and procedures on administrative levels and powers within the system and focus on the requirements of information security and its foundations (availability, safety and confidentiality).
3. Increase the financial budgets allocated to information security operations at the university.
4. The need for training and awareness of the importance of the system's information assets and the methods of maintaining them with a focus on the less experienced workers according to the results of the study.
5. Developing a strategic plan to manage the security risks of information systems, and ensuring the early detection of risks and the necessary preventive treatment.

References

Abdel-Gaber, Y. (2013). Effectiveness of internal control procedures in providing electronic information security in Jordanian industrial companies. Master of Accounting, Middle East University, Jordan.

Abdulkarim, N. (2013). The security and confidentiality of information and its impact on competitive performance applied study in the Iraqi public insurance companies and the red of civil insurance. Journal of Accounting and Financial Studies, vol. 8, p (23).

Abu, H., Sameh, R., & Abdeen, A. (2014). The role of IT governance mechanisms in reducing the risk of information security in government units under e-government. Research presented to the fifth annual conference, Cairo University.

Al-Buhaisi, EA. (2011). Freedom of Information Systems: An Empirical Study on Banks Operating in the Gaza Strip, Journal of the Islamic University, Series of Human Studies.

Al-Hadi, MM. (2006). Trends, security and transparency Information security in the shadow of e-government. Electronic Journal of the Arab Portal for Libraries and Information Cybrarians Journalhttp: //journal.cybrarans.org.

Al-Hanini, E. (2012). The Risks of Using Computerized Accounting Information Systems in the Jordanian banks -their reasons and ways of prevention. European Journal of Business and Management www.iiste.org. Vol . 4, No.20.

Al-Otaibi, AM. (2010). Information security in websites and its compatibility with local and international standards. Unpublished PhD thesis, Riyadh, Naif Arab University for Security Sciences.

Al-Salah, I. (2009). The Risks of the Security of Electronic Accounting Information Systems and their Impact on the Health and Reliability of Financial Statements in Jordanian Commercial Banks. Master Thesis published, University of Jordan, Amman.

Al-Salmi, AAR. (2001). Management Information Technologies. 1, Dar Wael Publishing, Amman.

Anton, R. & Mesic, RM. (2003). Finding and Fixing Vulnerabilities in Information Systems :The Vulnerabilities Assessment and Mitigation Methodology. Prepared for the Defense Advanced Research Projects Agency; National Defense Research Institute.

Awwad, NT. (2012). Effectiveness of the procedures of the internal control system under the electronic information systems - An applied study on the banks operating in the Gaza Strip. Master Thesis, Islamic University, Gaza Strip.

Danif, AM. (2013). The reality of the security management of information systems in the technical colleges in the Gaza Strip and ways to develop them. Master Thesis, Islamic University, Gaza.

Goodhue, D. & Straub, D. (2001). Security concerns of system users - A study of perceptions of the adequacy of security measures". Information and Management.

Heiser, G. (2013). Protecting e-Government Against Attacks. In : Proceedings of Security of e - Government Systems Conference. 19 February.

Irfan, SN., Abdul RM., Khaled, A. (2010). Information security in the Saudi organizations. King Saud University, Center for Excellence in Information Security.

Kissel, R. (2013). Glossary of Key Information Security Terms. NISTIR 7298 Revision 2, : National Institute of Standards and Technology (NIST).

Kreicbera, L. (2010). Internal Threat Information Security – Countermeasures and human factor within SME, Master Thesis, Sweden: Luela University Of Technology.

Litan, A. (2004). Phishing Attack Victims Likely Targets for Identity Theft. Gartner Research, Gartner, Inc. | FT-22-8873. USA.

Marianne, S. (2009). Security According to Buzan : A Comprehensive Security Analysis, security discussion. papers series 1. http://geest.msh-paris.

Merkow, B. & James (2005). Information Security : Principles and Practices, Prentice Hall.

Noordegraff, A. (2002). How Hackers Do it : Tricks ,Tools , and Techniques. U.S.A,CA : sun Microsystems ,INC.

Porter, B., Simon, J. & Hathrly, D. (2008). Principles of External Auditing, 3rd. edition, England.

Raval, V. & Fichadia, A. (2007). Risk, Controls, and Security : Concepts, Applications, England: John Wiley and Sons.

Romney, M. & Steinbart, P. (2012). Accounting Information Systems", 12th. edition, England : Pearson Education.

Sakaran, U. (2006). Research Methods for Business : A Skill Building Approach, 4th. Ed, Singapore : John Wily and Sons, (Asia) pte, Ltd.

Schechter, S. (2004). Computer Security Strength & Risk : A Quantitative Approach. PhD. dissertation, Computer Science, Cambridge: Harvard University.

Warkentin & Willison, R. (2009). Behavioral and policy issues in information systems security , the insider threat. European Journal of Information Systems.

Zuhairi, M.F. (2015). The Risks Facing The Security of Computerized Accounting Information Systems - A descriptive Study in Syrian Banks. master degree in Accounting.