Managing the Security of Information and Communication in Light of the Networks Technology

Raed J. Altoom

Palestinian , Jabalia, Gaza, Palestine

Altoomraed@gmail.com

Abstract— The research aims to manage the security of information and communication technology (ICT) systems in light of the networks within the IUG. The research concluded that there is a statistically significant relationship between the risks of the surrounding technology and systems security level according to of the population point of view that associated with natural disasters such as turning off the energy sources , fires and intentional disasters such as the Israeli attack on the infrastructure of information and communication technology (ICT). The study recommended to find a suitable alternative to manage and control the safety of the information system in and out the IUG to maintain the integrity of information, and the development of policies and procedures to protect the security information systems in the IUG, staff training on the latest technologies information by joining international conferences, learning from other experiences worldwide in addition to the commitment of senior management in the IUG in order to support the security information systems.

Keywords-component; management; information security; coomunication, networks

I. Introduction

The IUG is committed to the appropriate use of Information and Communication Technology (ICT) and Services in support of its teaching, research, administrative and service functions. The University acknowledges an obligation to ensure appropriate security for all Information and Communication Technology data, equipments, and processes in its domain of ownership and control. Every member of the University shares this obligation, to varying degrees. The IUG recognizes that successful implementation of ICT security relies on having well informed Users combined with effective management procedures.

Due to fast pace of change in ICT technology and its important applications, new security threats revolve around it. New and smart methods of information security are also devised by researchers to mitigate the risk occurred due to these threats. In the last decade process based information security management system(ISMS) such as ISO27001 and COBIT have emerged. Many organizations since then have adopted such ISMS. Knowledge Management(KM) is another management discipline enterprises employ, with aim to foster a more effective management of knowledge (Richard Y. K. Fung, 2008).

(IUG) makes use of information technology and communications (ICT), for instance, all the administrative, educational and registration issues are computerized through public networks. As shown in Table (1) in 2013,the number of registered students is 19241, while the number of the academic and administrative staff is 876 employee. The number of offered courses for the whole faculties is 1186.

1. TABLE. 1 The number of academic, students and administrative staff of the IUG*

2. university staff	3. Numbers
4. Academics	5. 413
6. administrator	7. 463
8. Students	9. 19,241
10. Total	11. 20,117

* According to the department of registration of the IUG)

Thus it becomes necessary to manage and protect the information. The network in IUG has like most of the communication networks weak access such as,the illegal use of the database information by students and employees. The separation between tasks and mandates of the employers. Moreover, it happened many time that, hackers penetrate the system….etc. Therefore, this research is concentrated for managing the security of information and communication in the network Technology in IUG. It becomes great interest providing necessary methods to protect information systems, control over their processes, ensure the sustainability of these systems correctly and in the required manner what it has been.

II. Problem of Research

The IUG experience in using the information technology in its systems communication internally and externally and securing high level of security to its networks from theft and illegal penetration, but in parallel the number of attacks and hackers to the IUG network are increasing. As it is well known, the security information and communication management is affected by many factors.

The research question: what are the factors that influence the management of information security and communications at the IUG?

.

III. RESEARCH VARIABLES

A. ***Dependent variable*** *The security of information and communication management*

B. . ***Independent variables***

The research independent variables including the following:

- Risks of input data
- Risks of output data
- Surrounding Technology
- Lack of experience and training
- Weakness of control procedure
- Policies and procedures

IV. RESEARCH HYPOTHESES

Main Hypothesis (1):

There is a statistically significant effect at (α=0.05) of the security information and communication management factors on the security of information and communication management

Sub-hypothesis:

H1a: There is statistically significant effect at (α=0.05) of risks input data on the security of information and communication management.

.**H1b:**There is statistically significant effect at (α=0.05) of risks output data on The security of information and communication management.

H1c: There is a statistically significant effect at (α=0.05) of surrounding on The security of information and communication management.

H1d: There is a statistically significant effect at (α=0.05) of lack experience and training on the security of information and communication management.

H1e: There is statistically significant effect at (α=0.05) of weakness of control procedure on the security of information and communication management.

H1f: There is a statistically significant effect at (α=0.05) of policies and procedures on the security of information and communication management

Main Hypothesis (2):

H1: There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to demographic characters (gender, age, experience, job title, qualifications).

Research objectives

The main goal of current research is to manage information and communication security in light of network technology at the (IUG), through the following objectives:

a) Determine the impacts of the input data risks on the security of information and communications in IUG.

b) Determine the impacts of the output data risks on the security of information and communications in IUG.

c) Determine the impacts of surrounding technology risks on the security of information and communications in IUG.

d) Determine the impacts of lack experience and training risks on the security of information and communications IUG

e) Determine the impacts of weakness of control procedure risks on the security of information and communications IUG

f) Determine the impacts of policies and procedures on information security and communications in IUG

g) To suggest recommendations that might help IUG in improving the security of information system in communications and networks technology.

The importance of research

a) This research interpreted modern and rapid developed technology, whereas any misleading results will lead to serious and high risk especially it concerns the information and networks management at the IUG.

b) Highlight most risks related to the inputs and outputs of the PC and the control procedures for systems at IUG.

c) Highlight the surrounding technology risks due to the human mistakes in the IUG and proposed procedures to limit that risks at IUG.

d) The need of the IUG to such research to minimize the risks of repeated penetrations and thefts through the system management to ensure the confidence of it.

e) The current research is a simple reference for any proposed research for the system at the IUG.

V. RESEARCH APPROACH AND METHODOLOGY

The methodology of this research is as follows

a) The study follows the procedure of a descriptive study. The researcher adapted analytical approach which depends on data collection, analysis using SPSS and interpretation of the results to determine the hypothesized relationships. The questionnaire was conduct to reach the result of the study

Primary Data: The research used the analytical descriptive approach and the comprehensive survey to introduce the research data in order to meet research objectives using the Statistical Package for the Social Sciences (SPSS). 72 questionnaires were distributed as a tool in survey the opinions of the research population, the collected questionnaires were (56) representing response rate (78%).

Secondary Data: This research depended on published and unpublished material such as referred journals, papers, text books and internal resources.

b) Questionnaire to ensure the proposed hypothesis, the target group were directors of the departments , heads of sections and all the staff of the information technology department.

Related Work

a) Definition of information security:

Information security is defined as policies, procedures and technical standards that are used to prevent unintentional access, theft or destruction of records (Sultan, 2009).

Information security is the protection of information and systems from unauthorized access, disclosure, modification, destruction or disruption. (Computing Services Information Security Office).

b) Information security objectives

According to Debi Ashenden,(2008) , the goal of information security must be consistent with the objectives of the organization, that to be necessary to achieve a set of requirements, which are:

Confidentiality: the privacy of customer information or the organization so that you are away from unauthorized access them to see it. Examples used for privacy encryption system, which is of important examples that provide a high level of security for information while maintaining the flexibility in the handling of such data.

Safety: and that includes making sure not display information and regulations for any kind of change is unauthorized, in other words, the data cannot be happening to her creation, change, or delete from the non-permit, and also means that the data stored in a parts database tables compatible with the corresponding data stored in another part of the databases. For example: you can miss the safety of the data in the database when a sudden interruption of electricity that feeds your server, or when you do not close the database correctly, and also because of deletion of information by mistake by a staff, may get bugs also due to a virus.

Availability: Availability of information and computer systems and security operations so that they work properly when you need it, and after the application of information security operations.

c) Elements of information security

The development of strategies and to find ways for the security of information and communication, and legislative measures in this regard, is to ensure the availability of the following items to any information intended to provide adequate protection to them, namely :(Sana Karim, 2008)

Privacy: and related to ensuring security and protection of data and information relating to individuals and companies from illegal access to it.

Ratification: which includes making sure that those who are using the data entry are the ones who appear on the network; ensure congruence between individuals who appear on the network and between individuals who are trying not to appear when they commit some mistakes.

Protection: Ensure that the data and information resources cannot be exposed to the illicit use by exposure to the violation by viruses or attacks by others outside the organization.

Confidentiality: means to make sure that the information is not disclosed nor seen it by persons not authorized to do so.

Authentication: This means making sure of the identity of the person who is trying to use the information and see if the user is correct that information or not, this is done by passwords for each user.

Integrity: which refers to making sure that the content of the information is true and is not modified or destroyed or tampered with in any stage of processing or exchange, whether dealing internally in the project or externally by unauthorized persons so is often done because illegal intrusions such as viruses where no one can break the Bank database and changes the account balance for that rests with the institution ensuring the safety of content through a suitable means of protection, such as software and hardware anti-breakthroughs or viruses.

Availability: built to ensure business continuity information system with all its components and the continued ability to interact with information and services for information sites and assure that the users of such information to prevent their use or accessed illegally undertaken by people to stop the service by a huge amount of absurd messages across the network to the institution's own devices.

Non-Repudiation: It is intended to ensure that the denial of a person who has performed a certain online information for this procedure, and therefore must provide a method or a way to prove any act done by any person for the person who has done at a certain time, for example, to make sure the arrival of merchandise was purchased via the Internet to its owner, and to prove transfer funds electronically is to use multiple messages such as e-signature and e-authentication.

d) Tools of information security:

The most important means of information security are (alshaaer, 2004).

Early detection of breakthroughs: The system registry file, and commands, and the operating system do this, and Task Manager, which displays all the programs and the program is recognized.

Network Protection: protect the network internally to take a series of actions, including the training of personnel in the network to deal with the security measures taken in the organization that contains the network.

Encryption arbitrator: to ensure that no unauthorized access to the system and the work schedule for re-encryption so it does not get its symbols to others, and the protection of electrical wiring and network extensions until one cannot break through it.

Firewall: The wall fiery software and hardware working on the nomination of data entering the database before it reaches the server and thus the firewall book up from the external network does not want to play in the internal network, and comes a firewall in the form of a wave brow Screening Router or in the form of more the effectiveness of such intermediary proxy so that he can understand the protocol used and interpreted.

Antivirus: a collection of programs that address the virus entering the device, and vary antiviral in terms of power and efficiency, but it can for virus makers and publishers exceeded effect often.

Multiple servers: It means multiple servers using server for each system or each group systems linked by a functional relationship, such as circulars, Transactions confidential, regulations and laws, investigations, wanted, Administrative Affairs, Public officers and individuals, as the presence of all these systems in a single server increases the likelihood of penetration and distribution of all systems and multiplicity leads to the decline of the problem in a single server and a single system.

VI. RESULTS

The research reached several findings:

a) There is statistical significant relationship between the risks on the surrounding technology and the level of system security from the point of view of the research population associated with natural disasters, fire, and Israeli attacks.

b) The impact of the surrounding technology on ICT security is significant which means that the system can be penetrated from outside.

c) The blockade prevents the imports of modern technology equipment to secure the system.

d) According to the research findings through the questionnaire respondents, the research concludes that there is lack of staff experience and training in the field of updated security programs, policies and procedures. In addition, there is dissatisfaction among the staff in the field of training especially in economic and social situation.

e) The research shows the risks associated with poor control procedures from the viewpoint of the respondents in the two elements are: the participation of the staff in using the same password and there is no clear policy forcing the staff to change the password periodically.

f) There is dissatisfaction among the staff in the field of economic and social situation.

g) Intercept and access data from servers to users' computers, because of the lack of knowledge of the mechanisms and their means of delivery, which requires improving access mechanisms.

h) Lack of adequate awareness among employees of the need to examine the new magnetic disks or programs when introduced to computers.

i) University administration benefit from the experience of international companies in the field of information security and communications.

j) The participation of staff in using the same passwords.

k) Differences among the research respondents' opinions: There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the research fields attributed to gender, age, level of qualification, specialization and the Governmental Institution.

VII. RECOMMENDATIONS

The IUG should prepare forms and clear standards rules to improve input data process.

The issue to look at skills needed to change organizational culture and identity of information security manager and effective communication between information securities manage and end user and senior manager. It should be clear that the classified document must be destroyed after use.

Reduce the risk of controls through the use of expertise and best practices in improving the levels of control procedures.

Monitor the communications of IUG to keep confidential information that is often easy to access and penetrate, by developing general policy of protecting the security of information, which clarify that the important information used by the staff, then to be destroyed after every use.

The senior management of IUG should be committed to the security program and support of information systems security continuously.

The information technology department responsible for the security of information systems should be provided with qualified staff with sufficient experience in information systems security.

Give interest in information security to IUG through the components of the networking technology and this to be improved continuously.

The research recommends training all employees to be more aware of security issues related to the system by clarifying the mechanisms to maintain data.

Develop procedures and policies to force the authorized employees “who have the authority to access and modify the data of the system”, to change their password periodically. Moreover, this model should be monitored and controlled to ensure that the system is secured and avoid stealing password.

The research recommends that not to allow the use of different kinds of storage media thereby to reduce the entry of virus into their systems in addition to do continuous updating of the antivirus software used by the university and set controls on the website to reduce the breakthroughs that could occur.

The research recommends that the IUG to hold and join international conferences regarding the ICT security, and to learn from other experiences worldwide. m) Raising awareness of chief executive officers of small businesses in information security management in Palestine.

The impact of training and education on information security and communications.

References

[1] Richard Y. K. Fung, (2008) , "Knowledge-Centric Information Security", International Conference on Security Technology, IEEE

[1] Sana Karim, (2008), "information security risk management: threats and protection," a paper presented to the Third International Forum on risk management strategy in institutions: Challenges and Prospects, held at the University of Chlef, Algeria Afqatrh 25-26 November.

[2] Ashenden, Debi, (2008), "Information Security management: A human challenge?", Information Security Technical Report, Vol.13, No.4: 195-201.

[3] Sultan, Abraham, (2009), "Management Information Systems: Systems Approach", University House for printing, publishing and distribution, Alexandria: Cairo.

[4] alshaaer, (2004), "Information and Communication Technology", publishing and authoring, Riyadh: Saudi Arabia.

[5] Computing Services Information Security Office (http://www.cmu.edu/iso/aware/presentation/tepperphd.pdf