Evaluating Protection of Computer Network in Education Sector

Yas A. Alsultanny

Abstract—**The use of Information Technology (IT) in the higher education institutes was increased daily. Most of the literature mentioned that the ISO/IEC 27002:2005 is the most popular standard to follow in order to reach the best protection for computer Networks. A questionnaire was designed to determine the extent of satisfaction with the level of production and to explore user's point of views regarding security. The questionnaire consists of 21 statements, according to the 5-points Likert scale. It was organized into 5 sections according to the most important factors. The data collected from 320 responds, they are users of the computer network in Arabian Gulf higher education sector. The results showed that the degree of information security in general at critical level. Security policy, access control, information security, incident management, and business continuity management are in acceptable level. List of recommendation was suggested to improve the computer network security in the higher education sector.**

Index Terms—**computer network, security, ISO/IEC 27002:2005, security management**

I. Introduction

Security is the process of protection systems from unauthorized usage. Unauthorized usage includes systems or data access by users who should have access to part of the system or database, but not all parts. The computer network protection is the acts of policies against unauthorized connectivity and distribution of privileges. The privileges must be distributed into levels to ensure computer network security.

According to the relative studies there were 1575698 database records had been unauthorized reviewed in 73 breaches at USA educational institute in 2010 [1]. Database system is an important core of any organization, especially in the field of education, which needs a computer network to access database by students, faculties, and employees, and now all the systems such as student registration, library, … etc., are build online on computer networks. These systems need a protection to maintain data from attacks, at the same time must be available to the users in a simple and fast form.

The ISO/IEC 27002:2005 (International Organization for Standardization/International Electro technical Commission) introduced 11 factors to protect the information and security management. In this paper some of ISO/IEC 27002:2005 (Code of Practice for Information Security Management) factors used to assess the degree of computer network security at Arabian Gulf universities. The successful management from any threaten to an organization computer security is a complex endeavor [2]. Therefore determining the exact requirements for security for any organization is essential for proper security to protect information systems from breaches [3].

This paper aims to evaluate protection of computer network in the higher education sector. The first section of this paper provides an introduction. The second section is for study motivations. The third section presents the research objectives. The fourth section is for related literature. The fifth section exhibits the research methodology. The sixth section describes data analysis. The final section is for discussion and conclusion.

II. Study Motivations

The motivations for this study emerge from the recommendations that appeared in the literature of computer network data security, which is the top priority for both governments and businesses worldwide, to keep personal financial and data in education sectors [4], [5]. The information security policy must be alignment with the organization strategy policy [6]. Information Systems Security (ISS) is a stream of management activities to protect the Information Systems. ISS have not only a technical part, but also a social dimension, that is a policy document [7]. It has become important for organizations to understand how to guard against hackers, outsiders, and even disgruntled employees who may threaten their information security [8].

A study focused on a 61 university which they have a security policy online on their sites, the results of this study recommended, that the security policy documentation is ―one of the first, if not the first, objective‖ for the universities [9]. Higher education institutions have experienced a substantially large number of data breaches – nearly 160 breaches and more than 2.3 million records breached during the years 2008 – 2010 in United States of America [10].

III. Research Objectives

The objective of this paper is to evaluate the protection of computer network in the Arabian Gulf higher education sector to keep their information in a secure and save method. This need to answer the following questions;

1. What is the level of *information protection incident management* in the higher education sector?
2. What is the level of *security policy* in the higher education sector?

3. What is the level of *business continuity management* in the higher education sector?
4. What is the level of *access control* in the higher education sector?
5. What is the level of *information system acquisition, development and maintenance* in the higher education sector?

IV. Related Literature

Network security is the protection of networking components, connections and contents, all of these need confidentiality, integrity and authenticity of protection, avoid other people or opponent use of wire-tapping, impersonation, tampering with, or deny, such as means of violating the interests of users and hidden, but also prevent other users of non-authorized access and destruction [11]. The introduction of networkable Windows-based operating system devices such as home entertainment systems, smart phones and Pocket PC, such devices introduced new challenges in terms of managing information security risks. In addition, these devices are vulnerable to information security threats because of the vendors and buyers lack of awareness of the security risks associated with such devices [12]. Threats are a set of circumstances that cause loss or harm, most of the threat to a computer system are; interception, interruption, modification, fabrication, weak audit trial, denial of service, backup data exposure, excessive privilege abuse, privilege evolution, platform vulnerabilities, and weak authentication [13]-[19].

No measurement for security, cause no control on database security [20]-[21]. It is importance of avoid the internal threat by well design a security policy, easy to read, easy to understand and easy to access, and let the entire user read it, in addition, create a user training and awareness program [22].

The extremely sensitive data must be stored in encrypted form [23]. Encryption consists of applying an encryption algorithm to data using some pre-specified encryption key. The resulting data has to be decrypt using a decryption key to recover the original data [24]. The computer network security depends onto the three basic requirements; confidentiality, integrity, and availability [25].

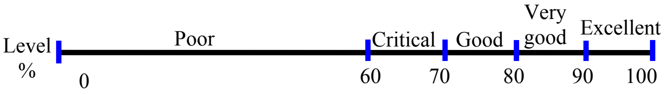
V. Research Methodology

Questionnaire was developed to implement the research of this paper based on previous studies in this field and on ISO/IEC 27002:2005 standard (www.iso.org). The questionnaire was delivered to specialists for evaluation. Then some modification on the questionnaire was taken place according to expert's suggestions. The final questionnaire consists of 21 questions based on 5-points Liekert – scale. The questionnaire divided into five sections according to the most important factors selected from ISO/IES 27002:2005.

The questionnaire designed to faculties, employees, and students in the Arabian Gulf higher educational sector. The questionnaire used to convert the respondents concepts into measurable variables. The total received respondents were 320, the study implemented in the academic year 2013-2014. The analysis was implemented by using SPSS version 19. The reliability factor measured by Cronbach's Alpha, it was equal to 0.84. Previous studies showed that if the value of Cronbach's Alpha equal or above 0.7 the data will be reliable [26]. The means and standard deviations were calculated, and the relative importance calculates by the following proposed scale:

$$\text{Relative importance} = [\text{mean} / \text{Top scale } (5)]*100 \tag{1}$$

The scale used to determine the level of the result is



The descriptive method was used to find the most important factors affecting on computer network protection.

VI. Result Analysis

The survey covers Arabian Gulf universities users (faculties, employees, under graduate students and graduated students). Fig. 1 shows the distribution of the total respondents according to their categorization.

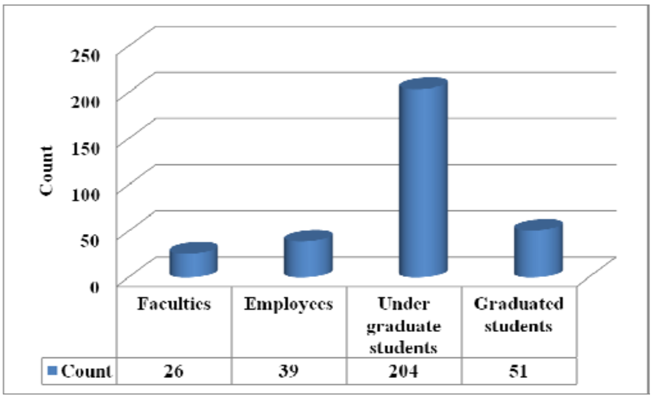


Fig. 1. Respondents' distribution according to category

Table I shows the results of the five factors concerning the questions of this paper. The "*information protection incident management*" factor got 66.96% of importance, the "*security policy*" factor got 66.81% of relative importance, the "*business continuity management*" factor got 65.86% of relative importance and "*access control*" got 60.89%, these three factors got the percentage between 60% and 70% and this means they are in critical level. Whereas the "*information system acquisition development and maintenance*" factor got 59.59% which is less than 60%, so this means that the factors are at poor level.

In general the level of the five factors is in critical level with percentage of 64.02%. This gives the answer of the objective of this paper that the protection level is at the critical level.

TABLE I
RELATIVE IMPORTANCE OF THE FIVE FACTORS OF THE PROTECTION LEVEL

No	Factors	Mean	Standard deviation	Relative importance %	Level
1	Information protection incident management	3.35	0.71	66.96	Critical
2	Security policy	3.04	0.83	66.81	Critical
3	Business continuity management	3.29	0.81	65.86	Critical
4	Access control	3.34	0.87	60.89	Critical
5	Information system acquisition, development and maintenance	2.98	0.88	59.59	Poor
Final score		**3.20**	**0.59**	**64.02**	**Critical**

In order to check the factors that have significant effect on the level of computer network protection, the mean and standard deviations calculated for each statement in each of the five factors (see Table I).

The first factor *information protection incident management* consists of five statements. Table II shows the results sorted downward according to the relative importance. The largest relative importance was 76.2% to the share of the responsibility of information protected according to users. In addition all other four statements were in critical level, with relative importance between 69.2% and 62.4%. The answer to the first question related to this factor is;

The level of *information protection incident management* in the higher education sector is at critical level with relative importance 67.00%.

TABLE II
RESULTS OF INFORMATION PROTECTION INCIDENT MANAGEMENT FACTOR

No	Statements	Mean	Standard deviation	Relative importance %	Level
1	As a user, I'm partially responsible of information protection at my university network	3.81	1.04	76.2	Good
2	I prefer to use my personal laptop at university, because I afraid that the university workstations are not fully protected	3.46	1.34	69.2	Critical
3	University network secure so that I do not loss my up loaded data	3.23	1.12	64.6	Critical
4	University network is secured to preventing my work station from attacking or any viruses	3.13	1.28	62.6	Critical
5	I have enough knowledge of the risks that can be caused by improper use of data	3.12	1.15	62.4	Critical
Final score		**3.35**	**0.71**	**67.00**	**Critical**

The second factor *security policy* factor consists of five statements. Table III shows the result of the statements are sorted down and according to the relative important, the largest level of the statement was good with relative importance of 77.2%, this related to performing the security policy. Whereas the lowest level of this factor was critical, with the relative importance was between 60.4% and 64.8%. The answer to the second question related to this factor is;

The level of *security policy* in the higher education sector is at critical level with relative importance 66.80%.

TABLE III
RESULTS OF SECURITY POLICY FACTOR

No	Statements	Mean	Standard deviation	Relative importance %	Level
1	I act upon security policy carefully when I use university systems to protect the network	3.86	1.12	77.2	Good
2	Security policy always signed once the user received the user name and password	3.24	1.28	64.8	Critical
3	There is a deterrent retribution to whose not accomplish the security policy and misuse the network	3.24	1.16	64.8	Critical
4	I have full Knowledge of the security policy items concerning IT system usage	3.02	1.28	60.4	Critical
Final score		**3.34**	**0.87**	**66.80**	**Critical**

The third factor *business continuity management* consists of four statements. Table IV shows the mean, standard deviations, relative importance and the level for each statement responds. The largest relative importance was 72.4% to sign-out my workstation when leaving. In addition all other four statements were in critical level, with relative importance between 67.8% and 60.0%. The answer to the third question related to this factor is;

The level of *business continuity management* in the higher education sector is at critical level with relative importance 65.86%.

TABLE IV
RESULT OF BUSINESS CONTINUITY MANAGEMENT FACTOR

No	Statements	Mean	Standard deviation	Relative importance %	Level
1	Sign-out my workstation from network when I leave university daily	3.62	1.33	72.4	Good
2	I stop using network if I noticed that there is a weakness in it for a limited period of time	3.39	1.07	67.8	Critical
3	University network work with highly performance when I need it	3.16	1.17	63.2	Critical
4	I can use the wireless network from anywhere at university and its protected and no one can tampered it	3.00	1.18	60.0	Critical
Final score		**3.29**	**0.81**	**65.86**	**Critical**

The *business continuity management* factor level was critical, which is relatively low. This is because of the followings:

- Users sign-out their workstations were at "good" level, this means not all the users sign-out. So the university needs to enforce the users to sign-out or let the system automatically sign-out, if the user not uses the workstation for a period of time.
- The university needs to enforce the users to stop using the network, if there is a weakness for a period of time, and add more effort for training and awareness of users.

- The network is not working with high level of performance at all times. This need to make the network in a high performance level.
- There is a weakness in wireless network, so the users are less satisfied in this service.

The fourth factor *Access control* factor consists of four statements. Table V shows the relative importance of each statement related to access control. The results showed that the user name has a higher relative importance according to user responds with 74.0% which is in a good level. The lowest relative importance was 43.8%, which is at poor level in the statement of changing password periodically. The final score gave a critical level, and this represents the minimum level of acceptance. The answer to the fourth question related to this factor is;

The level of *Access control* in the higher education sector is at critical level with relative importance 60.89%.

TABLE V
RESULTS OF ACCESS CONTROL FACTOR

No	Statements	Mean	Standard deviation	Relative importance %	Level
1	I have an active user name to enter my university network	3.70	1.36	74.0	Good
2	I always use my university network because I confidence the security and continuity of the network	3.21	1.22	64.2	critical
3	The privileges granted to me as far as my needs for study purpose.	3.08	1.31	61.6	critical
4	I change my password periodically	2.19	1.23	43.8	Poor
Final score		**3.04**	**0.83**	**60.89**	**critical**

The results of these factors agreed with the results of Carstens [27]. To increase the level of control access acceptance the following factors are recommend:

- Make sure that each user has an access to the university network.
- Changing passwords periodically by enforcing the user to change their password spatially at the beginning of each semester.

The fifth factor *information system acquisition, development, and maintenance* factor consists of four statements. Table VI shows that the information system acquisition, development and maintenance factor, are in poor level, this need attention and more effort in order to increase the level of relative importance. The largest level was to the share of data categorization with relative importance of 61.4%, which is almost close to poor level. In addition the other three statements got poor level with relative importance of 57.8%, 59.4% and 59.8%. The answer to the fifth question related to this factor is;

The level of *information system acquisition, development, and maintenance* in the higher education sector is at poor level with relative importance 59.59%.

TABLE VI
RESULTS OF INFORMATION SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE FACTOR

No	Statements	Mean	Standard deviation	Relative importance %	Level
1	The data categorized security according to colleges and departments, and it meets my requirements.	3.07	1.10	61.4	critical
2	My university provides me an enough space on university network to save any files securely.	2.99	1.21	59.8	Poor
3	My university data and their software are updated periodically.	2.97	1.11	59.4	Poor
4	My university provided the software on the network to download and use it on my workstation security.	2.89	1.16	57.8	Poor
Final score		**2.98**	**0.88**	**59.59**	**Poor**

The recommendations to improve this factor are;

- Add more effort in order to categorize the data according to college's and departments.
- Add enough space to users.
- Software needs periodically updating.

VII. DISCUSSION AND CONCLUSION

Computer network is one of the important tool used in the higher education sector, the faculty, employees, and students are using the university network to execute their jobs or for reading. To keep the database in a secure manner the database of the computer network must be kept securely. This paper evaluates the protection of computer network in the Arabian Gulf in the higher education sector to keep their information in a secure and save method. A questionnaire of 21, statements was distributed to three categories; faculty, employees, and students. The number of responds was 320. The percentage of 64.2% relative importance to the five factors was fall in the critical level, it was relatively low and it need more effort in order to increase the degree of computer network security, since it is very important in the higher education sector. The most important recommendations to improve the level of acceptance and to increase the user confidence are; users must be enforced to change their password at the beginning of each semester to increase the level of access control, a policy of security must be cleared to all users, and an increase awareness among users regarding the security by intensifying training or lectures

REFERENCES

[1] www.privacyrights.org, Privacy Rights Clearing House, retrieved 29 January 2014.

[2] A. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek, Incident Management Capability Metrics Version 0.1, Technical Report, CMU/SEI-2007-TR-008, ESC-TR-2007-008, CERT Program, 2007.

[3] A. Alshboul, Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks, Communications of the IBIMA, 2010. retrieved on 6 April 2014 from http://www.ibimapublishing.com/journals/CIBIMA/cibima.html

[4] S. Holovec, Database Encryption Solution using Empress RDBMS. Empress Software Inc., 2006.

[5] J. Shaul, “Implementing Database Security: Using Attack Analysis to Improve Your Defenses,” *Journal of Database Security*, vol. 7, pp. 18-20, 2008.

[6] N. F., Doherty, and H. Fulford, “Aligning the Information Security Policy with the Strategic Information Systems Plan,” *Journal of Computers* and *Security*, vol. 25, no. 1, pp. 55-63, 2006).

[7] M. Karyda, E. Kiountouzis, and S. Kokolakis, “Information Systems Security Policies: A Contextual Perspective,” *Journal of Computers & Security*, vol. 24, no. 3, pp. 246-260, 2005.

[8] S. K. Sharma, and J. Sefchek, “Ching Information Systems Security Courses: A Hands-on Approach,” *Journal of Computers and Security,* vol. 26, no. 4, pp. 290-299, 2007.

[9] N. F. Dohertya, L. Anastasakis, and H. Fulfordb, “The Information Security Policy Unpacked: A Critical Study of the Content of University Policies,” *International Journal of Information Management*, vol. 29, no. 6, pp. 449–457, 2009.

[10] Application Security Inc., An examination of database breaches at higher education’s institutions, 2010.

[11] J. Yan, Continuous Authentication Based on Computer Security. Unpublished Msc thesis, Luleå University of Technology, Department of Business Administration and Social Sciences, Sweden, 2009.

[12] I. Oshri, J. Kotlarsky and C. Hirsch, “Information Security in Networkable Windows-Based Operating System Devices: Challenges and Solutions,” *Journal of Computer & Security*, vol. 26, no. 2, pp. 177-182, 2007.

[13] S. L. Pfleeger and C. P. Pfleeger, *Security in Computing*, 3rd ed, prentice hall PTR, 2003.

[14] M. Smith, T. Friese, M. Engel and B. Freisleben, “Countering Security Threats in Service-Oriented on-Demand Grid Computing using Sandboxing and Trusted Computing Techniques,” *Journal of Parallel and Distributed Computing*, vol. 66, no. 9, pp. 1189-1204, 2006.

[15] A. Shulman, “Top Ten Database Security Threats - How to Mitigate the Most Significant Database Vulnerabilities,” *Trade Conferences*. Imperva, March 25th USA, 2006.

[16] G., V. Lioudakis, E., A. Koutsoloukas, N. L. Dellas, N. Tselikas, S. Kapellaki and G. N. Prezerakos, “A middle ware architecture for privacy protection, ” *journal of computer network*, vol. 51, no. 61, pp 4679-4696, 2007,

[17] L. Shinder, and M. Cross, *Facing the cybercrime problem head-on. in scene of the cybercrime*, 2nd ed, Syngress, 2008,

[18] K. Young, “Policies and Procedures to Manage Employee Internet Abuse,” *Journal of Computers in Human Behavior*, vol. 26, no. 6, pp. 1467-1471, 2010,

[19] O. Liu and Y. Zhang, VRSS: A New System for Rating and Scoring Vulnerabilities, Computer Communication, 2010.

[20] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty and Doubt*. Adison-Wesly Professional, 2007.

[21] T. K. Dang, T. H. Le and D. T. Truong, *An Extensible Framework for Database Security Assessment and Visualization*. Article, HCMC University of Technology, Department of Computer Science and Engineering, Vietnam, 2008.

[22] M. T. Arenas, Social *Engineering and Internal Threats in Organizations.* Unpublished Msc Thesis, School of Engineering Bleking Institute of Technology, Department of Computer Science, Sweden, 2008.

[23] E. Doyle, Lock up Your Data. *Journal of Infosecurity Today*, vol. 3, no. 4, pp. 31-33, 2006.

[24] K. C. Laudon and T. Guercio, *E-Commerce Business. Technology. Society,* 4th ed, Pearson Education Inc., 2010.

[25] E. R. Weippl, “Database Security and Statistical Database Security,” *Journal of Secure Business Austria*, pp. 610-616, 2009.

[26] J. Pallant, *SPSS survival manual*, 2nd ed, Bukingham: Open University press, 2005,

[27] D. Carstens, P. McCauley-Bell, and R. DeMara, “Evaluation of the Human Impact of Password Authentication Practices on Information Security,” *Informing Science Journal*, vol. 7, pp. 68-85, 2004.