SECURITY INFORMATION SYSTEM OF THE COMPUTER CENTER IN MU'TAH UNIVERSITY

Asma Jmeel Alnawaiseh
Mu'tah University

Abstract

The aim of this paper is to study the importance of security and protection at the computer center of Mu'tah University. In this study, we analyzed the following questions: Is security and protection a necessary requirement? What is the role management has applied to secure systems? What are the factors that have affected the security of any system? Finally, how can I secure my system after building it, and what methods can I use? Therefore, the data for this paper collected from the questionnaire was designed to achieve the stated objectives, and to encourage high response rate based on the questionnaire presented in international journals found on websites.

As for the structured interview, it was used to enrich the data collected by the researcher.

Keywords: Information, security, Mu'tah University, Jordan

Introduction

1. Background of Study

One of the management priorities today must be the establishment of data security plans, policies and programs for the corporate environment. However, management must be committed to participate in the design, installation and operation of all sensitive data systems.

New management personnel assist in this management function, and several key positions of these personnel includes: data security administrator, database administrator, disaster recovery manager, EDP auditor and copy manager. Therefore in small organization, one person might perform several of these roles; even as that, top management still has the responsibility for setting the overall guidelines for each function.

Basically, security does not only constitute data or information security, but also comprises of the physical ones such as: location, people and external environment security like the weather. Therefore, the main areas of enhanced security as mentioned earlier have been: firstly, physical

security embracing and fire security, and secondly, data and file security. So the importance of information system at Mu'tah university has become a very critical issues like in any other university and computer center because all department and colleges in universities has a computerized system, that requires information security and protection either internally and externally. As a result, this paper would give an in-depth study on these issues as well as the problems faced by the computer system at Mu'tah University.

However, the computer center was established in 1993 to provide computer services to all departments at Mu'tah University. This service includes:

- Operating and maintenance of the computer equipment.
- Developing and maintaining information systems.
- Supervision of all computerized exams in the university.
- Technical support for all pc's and network.
- Training for all university's staff and students.

2. Statement of the Problem:

We consider the problem of this research to be the answers to the following questions.

1. What are the importance of security and protection in our systems, and is it a necessary requirement?
2. What is the role management has applied to secure systems?
3. What are the factors that have affected the security of any system?
4. How can I secure my system after building it, and what methods can I use?

3. Significance of the study.

This study can provide the reader a good theoretical frame about the subject of the study. However, this would assist the reader to organize the importance of security issues concern for all fields and place a restriction on the main risks that threaded the information systems at our university. In addition, this study suggests the best solution for these systems, besides making survey about the opinion of employee themselves. At the end of this study, essential recommendation will be provided to improve the current system.

4. The Instruments of the Study.

The researcher designed a written questionnaire and an interview sheet. The questionnaire was designed to achieve the stated objectives and to encourage high response rate based on the questionnaire presented in international journals found on websites.

As for the structured interview, it was used to enrich the data collected by the researcher. Beside the fact that the employee of the computer center were given the opportunity to express freely what they thought about certain points, they were asked to respond orally to certain

questions.

5. Validity of the Instruments.

Candidate from two business colleges were involved in the pre-test of the questionnaire. 12 prototype of the questionnaire were distributed to 8 specialists, and it was only 3 of them that responded. Thus, some questions were dropped as response could not be easily given, while others were re-phrased for better interpretation.

6. Reliability of the Instruments.

The reliability of the questionnaire was found by distributing the questionnaire to 15 employees of the sample. However, to recognize the degree of clarity, it was computed using Crombach Alpha, and was found to be (.87) which is a suitable degree.

7. Data collection.

To collect the needed data of information security issues in all the departments that used information systems, two procedures were used: Structured Questionnaire and the interview**.**

8. Data Analysis.

The gathered data were analyzed statistically and descriptively. As for the statistical analysis, employee's responses on the questionnaires were computed and then analyzed using mean and standard deviation for the different dimensions of the questionnaire. In this study, the **SPSS (**statistical package for Social Sciences) software will be used, because it is easily available and easy to learn and understand. Furthermore, the methods employ frequency distribution to identify the percentage of responses of the sample, regression to test the hypotheses and the means and standard deviations (STDEV).

9. Hypotheses:

The first hypothesis: There are none committed to security principles, with the employee using information system.

The second hypothesis: There are none committed to system protection from personal risk, with the employee using information system at Mu'tah University.

The third hypothesis: There are none committed to system protection from physical risk, with the employee using information system at Mu'tah University.

The forth hypothesis: There are no significant relationship between the awareness of security and the demographic factors (Gender, Age, Experience, and Qualification) for the sample of this study.

10. Review of related literature

Scott (2001), with his article discuss the best steps that can be identified and taken, only when organization acknowledge and understand the real treats and the effective solution of IT security.

He defines the four real solutions that must be taken into consideration. They include: Security policy, Firewalls, Constant assessment and system administration responsible for security.

Tryfonans (2001), in his research focuses on strategic planning before building the secure system, and the information system security coming from external and internal producers inside and outside the system.

George (2002), at his article talks about how to secure systems against viruses using safety software like UNIX operating system because it is an ASCII files, and it uses updated antiviruses programs with making periodically updated.

Fulford and Doherty (2003), conducted a study to fill the gap between the information security issues and applied policy to achieve that security. They make exploratory investigation to investigate the uptake, content, dissemination and impact of information security policies. They mailed questionnaire to senior IS executives in large UK-based organizations, and 208 valid responses were received. The result of this research have indicated that while polices are now fairly common at least amongst the sample, there is still a high degree of variety in terms of their content and dissemination.

Simon(2003), studied the input flow tracing and its benefits such as the provision of matrices for security assurance, complete vulnerabilities assessment and the ability to examine combinations of vulnerabilities.

Victor_Valeriu Patriciu, Iustin Priescu, Sebastian Nicolase scu(2006)

Consequently, managing the security of enterprise information systems has become a critical issue in the era of the Internet economy. As any other process, security cannot be managed if it cannot be measured. The need for metrics is important for assessing the current security status, to develop operational best practices and also for guiding future security research. The topic is important at a time when companies are coming under increasing compliance pressures that require them to demonstrate due diligence when protecting their data assets. Therefore, metrics give companies a way to prioritize threats and vulnerabilities and the risks they pose to enterprise information assets based on a quantitative or qualitative measure. This paper presents a framework for ranking vulnerabilities in a consistent fashion, and some operational metrics used by large enterprises in managing their information systems security process.

Sattarova Feruza Y. and Prof.Tao-hoon Kim(2007)

Computer security is a branch of technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft,

corruption or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. There are many elements that are disrupting computer security. In this paper, we reviewed the current strategies and methods related to IT security.

Mathew Nicho, Shafaq Khan, (2014)

One of the most serious and persistent threat that has emerged in recent years combining technical as well as non-technical skills is the Advanced Persistent Threat, commonly known as APT. Here, hackers circumvent the organizational defenses and target the naivety of the employees in making an unintentional mistake.

While this threat has gained prominence in recent years, research on its cause and mitigation is still at the infancy stage. In this paper, the authors explore APT vulnerabilities from an organizational perspective to create taxonomy of non-technical and technical vulnerabilities. The objective is to enhance the awareness and the detection of APT vulnerabilities by managers and end users. To this end, the authors conducted interviews with senior IT managers in three large organizations in Dubai, United Arab Emirates. The analysis of the findings suggested that the APT threat environment is affected by multiple factors spanning from primarily nontechnical as well as technical vulnerabilities.

Methodology and Procedures

Style of the Study

In this study, there are several ways of obtaining information about security. They are:

- Collect the raw information from books and journals. Thus, some of these books are written by Arabic and foreign authors.
- Some articles and case studies can be taken from the internet provided by search engines (Google, Yahoo, Ebseco etc.), security site (www.itsecurity.com) and some information obtained from the computer center on the website of Mu'tah University.
- Observation of the applied system at the university by visiting the department and looking at the degree of security they possessed.
- The critical data collected by the questionnaire was designed to achieve the stated objectives and encourage high response rate, based on the questionnaire presented in international journals on websites.
- The important information gotten from interviews with the manger of security at the computer center and with the programmers that built the systems.
- Other data were obtained from personal experience and historical data

about the center and the security method they applied.

Findings of the Study

Findings of the Interview

In order to shed light on the security methods applied to the computer center, the researcher interviewed all the subjects and asked them the suitable questions they have listed. After analyzing their answers, the researcher came up with the following findings about the information security and protection department at the computer center.

1. They established a policy and producers that prevent any illegal access to data and information, so only the employee who is responsible for it can access the systems.

2. Daily backup made at 8 o'clock every morning.

3. Tracking the change that occurs on the system or database (if any change was discovered).

4.They established isolated room called the site, where nobody enters without permission, but the operator only, to carry out his operational activities on the servers every day and creating backup for all the systems.

5. They keep the backup tapes at safety location in the site room.

6. No one can make any copyright of any software in the center.

8. They have alarm system, air condition and they separately distributed the PC's inside the center.

9. Anti-virus and firewalls were installed on the servers.

10. The password was distributed to the site employee only, like this:

- **Sun server and proxy server:** security manager, Engineer of site and Employees of site**.**
- **Compaq server**: security manager, Engineer of site and Employees of site**.**
- **Alpha, vax and dec2**: security manager, IT manager and Employees of site**.**
- Dell **server**: security manager, Engineer of site and Employees of site**.**

Findings of the Questionnaire.

As mentioned previously by the researcher, the gathered data was statistically analyzed using the Statistical Package for Social Sciences known as SPSS. However, the methods used were frequency distribution, Regression, standard deviation and the means.

1. Description of the Sample.

Table (1)The Proprieties of the Sample

Variable		Number	Percentage 0/0
Gender	Male	63	78.8
	Female	17	21.2
The age	20-25	15	18.8
	26-30	33	41.3
	31-35	9	11.3
	36-40	18	22.5
	>40	5	6.3
Experience	<5 years	13	16.3
	6-10 years	41	51.3
	11-16 years	5	6.3
	17-20	18	22.5
	>20 years	3	3.8
Qualification	Secondary &diploma	12	15
	Bachelor degree	60	75
	High education	8	10

- From the last table, we can notice that the number of female in our sample is 63 or 78.8%; on the other hand, the female employee was 17 and 2l.2.
- The age between (26-30) is the high percentage 41.3%, the second percentage is 22.3% for the age between (36-40), the low percentage is for the age greater than 40%, and hence the percentage is 6.3%.
- The distribution of the sample on experience factor; the high percentage for (6-10) years was (5l.3 %), on other side, for the lowest percentage greater than 20 years, the percentage was 3.8%.
- The most sample were from bachelor degree, the percentage was 75% and the number was 60 employees, the less percentage was for high education 10%.

The means and the standard deviation.

To determine the trends of employee, the means was calculated as shown in **table (2).**

Table (2) The Mean

Strongly agree	**Agree**	**Neutral**	**Strongly Disagree**	**Disagree**
5	4	3	2	1

So if the mean is less than 3, it indicates negative response; and if it is greater than 3, it indicates a positive response for that factor.

Table (3)The Means and STDV for Awareness ofInformation Security

No	**The Mean**	**STDV**
2	3.062	1.14
3	2.312	1.07
4	2.215	1.12
5	3.025	1.36
6	3.037	1.23
7	3.220	1.13
8	3.275	1.11
9	3.087	1.11
10	3.10	1.23
11	3.231	1.32
Total	**2.920**	

As shown in **table (3),** we can indicate that the awareness of security issues (information and physical one) by Mu'tah University employee is a negative trend. However, it requires much effort to create awareness for the employee, and explaining to them the importance of security to their information.

Total Table (4) The Means and STDV for Personal Risk

No	**The Mean**	**STDV**
12	2.96	l.14
13	3.23	l.24
14	2.88	1.11
15	2.78	l.02
16	2.46	l.21
17	2.82	l.17
18	3.07	l.38
19	2.86	l.09
20	2.92	l.11
21	2.76	l.07
Total	**2.87**	l.14

As shown in table (4), we can indicate that the personal risk by Mu'tah University employee is a negative trend. So, it requires making much effort in developing and training the employee to become more effective. In addition, it also entails placing regulation to punish any careless employee

that compromises the rules.

Table (5) The Means and STDV for Physical Risk

No	The Mean	STDV
22	3.187	1.14
23	2.7	1.24
24	2.93	1.11
25	2.88	1.02
26	2.92	1.21
27	2.92	1.17
28	2.81	1.38
29	2.81	1.09
30	2.55	1.11
31	2.55	1.07
Total	**2.84**	

As shown in **table (5),** we can indicate that the employee trend to physical security at Mu'tah University is a negative trend and **the total mean (2.84).** So, it requires making much effort to secure the location and the external factors that may be affecting the security of information.

3 Hypotheses test:

By using the regression test, the founded results were:

Hypothesis 1: There was no awareness of security principles on the use of information system by the Mu'tah University Employees.

Table (6) The test result for first hypothesis

Sig	F	Means square	D.f	Sum of squares	Model
.982	.001	6.865	1	6.865	Regression
		1.369	78	106.799	Residual
			79	106.800	Total

R=.003

From the above table, we accepted the (zero hypothesis at Sig .982), which signifies that there are no awareness of security issues by Mu'tah University employee.

Hypothesis 2: There are none committed to protect the system from personal Risk through the Employee use of information system at Mu'tah University.

Table (7) The test result for second hypothesis

Sig	F	Means square	D.f ,I	Sum of squares	Model
.253	1.324	1.783	1	1.783	Regression
		1.346	78	105.017	Residual
			79	106.800	Total

R=.260

From the above table, we accepted the (zero hypothesis at Sig .253), which signifies that there are no commitment from Mu'tah employee to keep their systems from personal risk.

Hypothesis 3: There are none committed to protect the computer system from Physical risk with the employee use information system at Mu'tah University.

Table (8) The test result for third hypothesis

Sig	F	**Means square**	**D.f**	Sum of **squares**	**model**
.020	5.639	7.20	1	7.20	Regression
		1.277	78	99.60	Residual
			79	106.800	Total

R=.260

From the above table, we accepted the (Null hypothesis at Sig .020), which signifies that there are no commitment from Mu'tah employees to keep their systems from physical risk.

Hypothesis 4: There are no significant relationship between the awareness of security and the demographic factors (Gender, Age, Experience, and qualification) for the sample of this study.

To test this hypothesis, the (ANOVA) test was used and the result is as show below in **table (9).**

Table (9) The Result of ANOVA Analysis for Fourth hypothesis

Sig	F	**Variable**
.381	.776	Gender
.224	1.465	Experience
.594	.700	Age
.189	1.703	Qualification

So from the table above, we discovered that there are no significant relationship between the awareness of security and the demographic factors (Gender, Age, Experience, and qualification) for the sample of study. However, we rejected the null Hypothesis.

Conclusion

This final part of the study summarizes the research carried out, including the key finding and their implications. Thus, there are lots of recommendations which must be taken into considerations when building a secured information system (physically and logically). For physical security, every employee should be provided with a magnetic card accompanied with a password to enter the center through only one auto door. In addition, spare UPS should also be provided beside the main ones. The responsibility about security and protection issues should be clearly defined with punishing and

rewarding system; and also, training and development on security should be given to employees. However, for information security, the following is recommended: using proper documentations for all the system they build, using profiles to keep track of employee movement among the System or program, filtering the web site which is accessed by the students. Others includes operating the backup files on the (spare server) to check its validity, using strong operating system like Unix, which enable mirror images to be sent automatically to another servers, making encrypted data and password and terminating the time for the passwords after the employee leaves the job or is being paid-off. Therefore, in all the systems, the programmer must create permission table, with 5 different levels to be able to access the programs. Furthermore, to ensure network security, the following should be used: firewall system, packet filter, or performs any reverse proxy Function, and User identification and authorization (files & devices). Also, encrypted data and messages through the network should be used. Finally, more research should be done about this topic, because there are great deals of Arabian books and articles about information security. In addition, Mu'tah University should organize more meetings on the security issues, and also encourage their employee to participate in any activity related to security and protection information systems, like security conferencing and lectures at the university.

References:

Dimitrion.S, Identify Security vulnerabilities through input flow tracing and analysis. Information management &computer security journal ,vol 11, pp 195-199 2003.

Fulford .H ,Neil F Doherty (2003) , The application of information security policies in large UK –based organization :an exploratory investigation . Information management &computer security journal ,vol 11 pp 106-114,. 2003.

George C . Smith (2002) Anti-virus protection ,intrant journal 29/10/2002

Kopparapu. C(2002) Load balancing servers Firewalls and caches. USA ,wiley computer publishing

Mathew.N,Shafaq.K, Identifying vulnerability of advanced persistent threats: an organization perspective. International journal of information and privacy,8(1),1-18,january_march 2014 1

Sattarova Feruza Y. and Prof.Tao-hoon Kim, IT security review privacy, protection, access control assurance and system security, International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No.2, 2, April, 2007.

Tryfounans. T (2001) ,embedding security practices in contemporary information system development approaches . Information management &computer security journal ,vol 9 No4 pp183-197.