CHAPTER IV

RESEARCH RESULTS

4.1 INTRODUCTION

This chapter presents the data analysis based on data that have been collected from staff in G.O.A.L.S on the information security risk involving e-learning systems. The research involved the development of a questionnaire to identify the perception of respondents on unauthorized release of information, unauthorized modification of information, unauthorized denial of resource use. The data collected through questionnaire were processed by SPSS software and presented in frequency tables for the benefit of answering the research objectives.

4.2 RESPONDENTS' CHARACTERISTICS

There were initially ten populations of staff in G.O.A.L.S USIM, N=10. Only 8 of them managed to complete the questionnaire that is the number of respondent is eight which means our sample size is 8.

4.2.1 Gender

Table 4.1 shows that most of the respondents were male (62.5%) and Female were 37.5%.

Table 4.1: Gender

	N	%
Male	5	62.5
Female	3	37.5
Total	8	100.0

4.2.2 Education Level

Table 4.2 shows that half of the respondent has Bachelor Degree, while 37.5% has Diploma. Only one (12.5%) respondent has Doctorate Degree.

Table 4.2: Education Level

Level	N	%
Diploma	3	37.5
Bachelor Degree	4	50
Master Degree	0	0
Doctorate Degree	1	12.5
Total	8	100.0

4.3 DESCRIPTIVE ANALYSIS OF QUESTIONNAIRE

There are three risk categories of information security studied that are unauthorized release of information, unauthorized modification of information and unauthorized denial of resource use. This questionnaire was scored using the Likert scale; from Yes, Not Sure and No, (1 – 3).

4.3.1 Unauthorized Release of Information

The first section is unauthorized release of information that consists of 10 items (refer Table 4.3 represents the descriptive measure of the Likert scale for this first section. Item 1 to item 5 indicated than all of the respondents answered No to the item, while the last 5 items one respondent (12.5%) answered Not Sure and others answered No (87.5%).

Table 4.3: Descriptive Statistics of Unauthorized Release of Information

No	Item	Yes	Not Sure n (%)	No
1	Logon information of lecturers were intercepted and misused.	-	-	8 (100%)
2	Logon information of students were intercepted and misused.	-	-	8 (100%)
3	Materials online were loaded by unauthorized persons.	-	-	8 (100%)
4	Materials online were accessed by unauthorized users.	-	-	8 (100%)
5	Materials online were phished by unauthorized persons.	-	-	8 (100%)
6	Students get unauthorized person's help during the writing of tests.	-	1 (12.5%)	7 (87.5%)
7	People masquerade as students to answer tests on behalf of such students.	-	1 (12.5%)	7 (87.5%)
8	Hackers managed to access the system.	-	1 (12.5%)	7 (87.5%)
9	Crackers managed to destroy the system.	-	1 (12.5%)	7 (87.5%)
10	Virus or Trojan managed to attack the system.	-	1 (12.5%)	7 (87.5%)

4.3.2 Unauthorized Modification of Information

In the second section, unauthorized modification of information has 10 items (refer Table 4.4) represents the descriptive statistics for unauthorized modification of information. None of them answered Yes to all of the items in this section. All of them answered No to 'materials were ruined' and 'assignments sent by students were lost' (100%). Thirty-seven per-cent answered Not Sure to item 1, 4, 5, 9 and 10 and remaining 62.5% answered No. One respondent answered Not Sure in item 3 and 8. Half of respondents answered Not Sure and No in item 7.

Table 4.4: Descriptive Statistics of Unauthorized Modification of Information

No	Item	Yes	Not Sure	No
			n (%)	
1	Materials online were changed by unauthorized person.	-	3 (37.5%)	5 (62.5%)
2	Materials online were ruined.	-	-	8 (100%)
3	Materials online were lost.	-	1 (12.5%)	7 (87.5%)
4	Assignment sent by students was plagiarised by unauthorized person.	-	3 (37.5%)	5 (62.5%)
5	Assignment sent by students was ruined.	-	3 (37.5%)	5 (62.5%)
6	Assignments sent by students were lost.	-	-	8 (100%)
7	Student's marks were changed by unauthorized person.	-	4 (50%)	4 (50%)
8	Student's marks were ruined.	-	1 (12.5%)	7 (87.5%)
9	Student's marks were lost.	-	3 (37.5%)	5 (62.5%)
10	Quiz/test content uploaded by lecturer were changed.	-	3 (37.5%)	5 (62.5%)

4.3.3 Unauthorized Denial of Resource Use

There were 10 items in the third section, unauthorized denial of resource use (refer Table 4.5) represents the descriptive statistics for unauthorized denial of resource use. Majority of the respondents answered No in item 3, 4, 6, 9 and 10. Majority of them answered Not Sure in item 1, 5 and 7. One respondent answered Yes in item 3, 4, 7, 8, 9 and 10.

Table 4.5: Descriptive Statistics of Unauthorized Denial of Resource Use

No	Item	Yes	Not Sure	No
		n (%)		
1	Lecturers cannot access the system due to poor bandwidth.	2 (25%)	4 (50%)	2 (25%)
2	Students cannot access the system due to poor bandwidth.	2 (25%)	3 (37.5%)	3 (37.5%)
3	Lecturers cannot access the system due to server problem.	1 (12.5%)	1 (12.5%)	6 (75%)
4	Students cannot access the system due to server problem.	1 (12.5%)	-	7 (87.5%)
5	Lecturers could not log in to the system due to other reasons.	2 (25%)	4 (50%)	2 (25%)
6	Students could not log in to the system due to other reasons	2 (25%)	-	6 (75%)
7	Lecturers get disconnected when uploading or downloading materials in the system.	1 (12.5%)	4 (50%)	3 (37.5%)
8	Students get disconnected when accessing online materials or conducting quiz/test.	1 (12.5%)	3 (37.5%)	4 (50%)
9	Lecturers could not upload or download files in the system.	1 (12.5%)	1 (12.5%)	6 (75%)
10	Students could not upload or download files in the system.	1 (12.5%)	1 (12.5%)	6 (75%)

4.4 RISK ASSESSMENT

Risk assessment seeks to determine the causes of this danger and there are basic steps proposed by Rausand (2013) as follows:

1. In this step is to determine if the risk is intentional or unintentional. It is from Insider or Outside, Software, Hardware, Antivirus, Spy, Trojan, SQL and others. These risks are also classified in terms of whether or not they will provide the effect of fabrication, modification, interruption or interception to the information and also decide who might be harmed, or not and how.
2. Evaluate the risk and decide on precautions: In this step is to know the security vulnerabilities for application employed for the e-learning and the extent of damage resulting from this risk.
3. Record the findings and implement them: When the administrator know the type of risk and damage resulting from it, then it can take the appropriate decision against this threat or minimize damage.
4. Review the assessment and update if necessary: Review, then carry out an assessment and updates the system, and learn from mistakes or flaws in the previous system (Rausand, 2013).

Information security risk assessment was conducted for this research according to Rausand (2013) and the results as shown in the following sections.

4.4.1 Risk Assessment Step 1: Determine Information Security Threats

Researcher has divided information security threat source from the data collected into 2 categories as outlined by Jouini et al. (2014) that are Human and Technology. However, the third category that is Environmental Factors is not included in this study.

4.4.1.1 Human Threats

Table 4.6 showed the results for information security threats involving human. The results showed that 100% of the respondents chose No to all type of threats. However, a number of respondents answered Not Sure to 10 threats from the total of 16 threats. The lowest is 1 respondent for Student's marks were ruined, Students get unauthorized person's help during the writing of tests, People masquerade as students to answer tests on behalf of such students, Hackers managed to access the system and Crackers managed to destroy the system. Then, followed by 3 respondents for Assignment sent by students was plagiarized by unauthorized person, Assignment sent by students was ruined, Materials online were changed by unauthorized person and Quiz/test content uploaded by lecturer were changed. Lastly, there were 4 respondents for Student's marks were changed by unauthorized person. Apparently, with this result, human treat does not have negative impact on the system because Not Sure could not be considered as information security threats to GOALS.

Table 4.6: Descriptive Statistics of Human Threats

No	Item	Yes	Not Sure	No
		n (%)		
1	Logon information of lecturers were intercepted and misused.	-	-	8 (100%)
2	Logon information of students were intercepted and misused.	-	-	8 (100%)
3	Student's marks were ruined.	-	1 (12.5%)	7 (87.5%)
4	Materials online were loaded by unauthorized persons.	-	-	8 (100%)
5	Materials online were accessed by unauthorized users.	-	-	8 (100%)
6	Materials online were phished by unauthorized persons.	-	-	8 (100%)
7	Students get unauthorized person's help during the writing of tests.	-	1 (12.5%)	7 (87.5%)
8	People masquerade as students to answer tests on behalf of such students.	-	1 (12.5%)	7 (87.5%)
9	Hackers managed to access the system.	-	1 (12.5%)	7 (87.5%)
10	Student's marks were changed by unauthorized person.	-	4 (50%)	4 (50%)
11	Crackers managed to destroy the system.	-	1 (12.5%)	7 (87.5%)
12	Assignment sent by students was plagiarized by unauthorized person.	-	3 (37.5%)	5 (62.5%)
13	Assignment sent by students was ruined.	-	3 (37.5%)	5 (62.5%)
14	Materials online were changed by unauthorized person.	-	3 (37.5%)	5 (62.5%)
15	Materials online were ruined.	-	-	8 (100%)
16	Quiz/test content uploaded by lecturer were changed.	-	3 (37.5%)	5 (62.5%)

4.4.1.2 Technological Threats

Table 4.7 showed the results for information security threats involving technology.

There were 10 threats identified for this study where respondents have answered Yes

in the questionnaire. The lowest is 1 respondent for Lecturers cannot access the system due to server problem, Students cannot access the system due to server problem, Lecturers get disconnected when uploading or downloading materials in the system, Students get disconnected when accessing online materials or conducting quiz/test, Lecturers could not upload or download files in the system and Students could not upload or download files in the system. Then, followed by 2 respondents for Lecturers cannot access the system due to poor bandwidth, Students cannot access the system due to poor bandwidth, Lecturers could not log in to the system due to other reasons and Students could not log in to the system due to other reasons. Therefore, with this result, technological treats does have negative impact on the system and can be considered as information security threats to GOALS.

Table 4.7: Descriptive Statistics of Technological Threats

No	Item	Yes	Not Sure	No
		n (%)		
1	Assignments sent by students were lost.	-	-	8 (100%)
2	Student's marks were lost.	-	3 (37.5%)	5 (62.5%)
3	Materials online were lost.	-	1 (12.5%)	7 (87.5%)
4	Virus or Trojan managed to attack the system.	-	1 (12.5%)	7 (87.5%)
5	Lecturers cannot access the system due to poor bandwidth.	2 (25%)	4 (50%)	2 (25%)
6	Students cannot access the system due to poor bandwidth.	2 (25%)	3 (37.5%)	3 (37.5%)
7	Lecturers cannot access the system due to server problem.	1 (12.5%)	1 (12.5%)	6 (75%)
8	Students cannot access the system due to server problem.	1 (12.5%)	-	7 (87.5%)
9	Lecturers could not log in to the system due to other reasons.	2 (25%)	4 (50%)	2 (25%)

10	Students could not log in to the system due to other reasons	2 (25%)	-	6 (75%)
11	Lecturers get disconnected when uploading or downloading materials in the system.	1 (12.5%)	4 (50%)	3 (37.5%)
12	Students get disconnected when accessing online materials or conducting quiz/test.	1 (12.5%)	3 (37.5%)	4 (50%)
13	Lecturers could not upload or download files in the system.	1 (12.5%)	1 (12.5%)	6 (75%)
14	Students could not upload or download files in the system.	1 (12.5%)	1 (12.5%)	6 (75%)

As for the data analysis, the information security threats faced by GOALS will be considered when the respondents answered Yes in the questionnaire. Therefore, 6 threats have been identified as in Table 4.8.

Table 4.8: Information Security Threats in GOALS

No	Item	Effect to Information	Who is being Harmed
1	Lecturers/students cannot access the system due to poor bandwidth.	Interruption	Lecturers and students cannot access GOALS.
2	Lecturers/students cannot access the system due to server problem.		
3	Lecturers/student could not log in to the system due to other reasons.		
4	Lecturers/students could not upload or download files in the system.	Interception	Lecturers cannot upload/download files/materials for their course.
5	Lecturers get disconnected when uploading or downloading materials in the system.		
6	Students get disconnected when accessing online materials or conducting quiz/test.		Students cannot download materials and take quiz/test for their course.

Based on Table 4.11, information security threats in GOALS have two types of effect to information that are Interruption and Interception as classified by Rausand (2013). Interruption here involved problems where lecturers and students cannot access GOALS either due to poor bandwidth, server problem or other reason. Meanwhile, Interception involved problems of uploading or downloading files or materials by lecturers or students and also problems that occurred when students answered online test or quiz.

4.4.2 Risk Assessment Step 2: Risk Evaluation

The purpose of this step is to identify what could go wrong (likelihood) and what is the consequence (loss or damage) of it occurring. This step is important to determine the vulnerabilities and damage caused by the attack.

Table 4.9: Risk Evaluation of Information Security Threats in GOALS

No	Item	Vulnerability	Damage
1	Lecturers/students cannot access the system due to poor bandwidth.	Web-based application vulnerability	Denial of service
2	Lecturers/students cannot access the system due to server problem.		
3	Lecturers/student could not log in to the system due to other reasons.		
4	Lecturers/students could not upload or download files in the system.	Content vulnerability	
5	Lecturers get disconnected when uploading or downloading materials in the system.		
6	Students get disconnected when accessing online materials or conducting quiz/test.		

Table 4.9 shows the risk evaluation of information security threats in GOALS. There were two types of vulnerabilities that affect the system, which were Web-based application vulnerability as mentioned by Atashzar et al. (2011) and Content vulnerability as mentioned by Derawi (2014). Web-based application vulnerability involvedproblems where lecturers and students cannot access GOALS either due to poor bandwidth, server problem or other reason. Meanwhile, Content vulnerability involved problems of uploading or downloading files or materials by lecturers or students and also problems that occurred when students answered online test or quiz. Both of these vulnerabilities lead to one main damage to GOALS that is Denial of service, as classified by Jouini et al. (2014).

4.4.3 Risk Assessment Step 3: Proposed Remedies for Information Security Threats

Remedies for information security threats are important to prevent further damage to the e-learning system and avoid the same threat or other threats in the future. Table 4.10 proposed remedies against information security threat in GOALS.

Table 4.10: Proposed Remedies for Information Security Threats in GOALS

No	Risks	Remedies of Risks
1	Lecturers/students cannot access the system due to poor bandwidth.	Access control using firewall
2	Lecturers/students cannot access the system due to server problem.	
3	Lecturers/student could not log in to the system due to other reasons.	
4	Lecturers/students could not upload or download files in the system.	
5	Lecturers get disconnected when uploading or downloading materials in the system.	
6	Students get disconnected when accessing online materials or conducting quiz/test.	

Based on Table 4.10, the proposed remedy for all information security threats in GOALS is by implementing access control using firewall, this remedy also support Barik & Karforma (2012). A firewall is a blend of equipment and programming security system secured to avert unapproved access to a corporate system from outside the organization. Main principle is that all movement from inside to outside and the other way around must go through the firewall. To achieve this, all access to the local network must first be physically blocked, and access only via the firewall should be permitted. Only the traffic authorized as per the local security policy should be allowed to pass through. The firewall itself must be strong enough to be well secured. In order to achieve this, the bandwidth and server of the institution must be strong and always running for 24 hours without any interruption. The operation of the system must be well secured too by applying advanced malware detection, which is crucial to institution defense. An institution must learn how to defend one's network and data against malware. With all these in place, the lecturers and students will be able to access the system, upload and download necessary materials without any interruptions.

4.4.4 Risk Assessment Step 4: Review the Assessment

The rapid development in technical areas and ongoing competition between companies could lead to new threats. So it makes sense to review what have been conducted on an ongoing basis to improve the protection of the e-learning system. In reviewing the assessment, it involves the identification of what, why, where, when and how events or situations could either harm or enhance the ability of the institution to achieve its objectives. All of these things help us to get good results in terms of maintaining the system of all threats.

5. SUMMARY

The staff of goals center were very sure that material or information that are loaded are secured. However, there is some problem of interruption to access the system by lecturers and students due to poor bandwidth, server problem and other reason. Then, it also involves interception to the system that disable or disconnect lecturers or students when they upload or download files in the system, and also when student conduct quiz or test.