

INFORMATION SECURITY RISK ASSESSMENT OF
E-LEARNING SYSTEMS: A CASE STUDY OF GLOBAL
OPEN ACCESS LEARNING SYSTEM IN
UNIVERSITI SAINS ISLAM MALAYSIA

MOHAMED MUHSIN SALEH KANSUR

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

UNIVERSITI SAINS ISLAM MALAYSIA

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own, except for quotations and summaries which have been duly acknowledged.

Date: 28 July 2015

Signature:

Name: Mohamed Munser Saleh

Matric No: 3130152

Address: 22-14 Permai Puteri, Jalan 13 D,
Desa Permai, Taman Dato Ahmad Razali,
Ampang 86000 Selangor .

BIODATA OF AUTHOR

Mohamed Munser Saleh Mansour (M3130152) was born on the 30 March 1976 in Libya. He is Libyan and Passport No is (206937). He previously was a student of High Institute for preparation of Trainers in Zleettin and graduated in 1997 from Electronic Engineering Division\Computer. He was the Head of Graduated Student Unit at the Higher Institute for Comprehensive Alqrbolli Careers in the period (2004-2007). He was also the head of the Department of Students Activity and Trainer at the Higher Institute for Comprehensive Alqrbolli Careers in the period (2008-2012). He is at present a Master student of Universiti Sains Islam Malaysia (USIM) majoring in Computer Science of Information Security and Assurance (ISA).

ACKNOWLEDGEMENTS

I am very glad to write this page with great thanks to Allah Almighty, who gave me ability to complete my master degree in Computer Science of Information Security and Assurance.

This master's thesis was written in 2014 at Faculty of Science and Technology at Islamic Science University of Malaysia.

First of all I wish to express my sincere gratitude to my supervisor Dr. Fauziah Abdul Wahid for her great support through doing this thesis. I have got from her, motivations and a lot of useful feedback. I wish her a great success in her academic career even in her different life's aspects.

It was also an honor to be able to study Information Security and Assurance at USIM University. I want to especially thank Prof. Dr. Kamaruzzaman Seman, Dr. Najwa Hayaati Alwi, Prof. Emeritus Dr. Jalani Sukaimi, Dr. Madihah Binti Mohd Saudi, Dr. Mohammad Nasrin, Dr. Kamarudin Saadan, Dr. Madihah Mohd. Saudi, Dr. Nurlida Basir, Prof. Dr. Norita Md. Norwawi, Dr. Mohammed Zalisham, for teaching me and providing me a lot of support in the field of information security.

I wish to express my debt to all USIM's staff and all my sincere colleagues in FST for the useful discussion we had during our study.

With my sincere thanks for Cultural Attaché Office - Embassy of the Libyan in KL.

Finally, I dedicate this work to my sincere parents, all my family members, my wife, my sons, all my brothers, sisters and my friends, for their support to me. Without forget my country Libya.

ABSTRAK

Kajian ini menyiasat masalah risiko keselamatan maklumat yang berkaitan dengan sistem E-Pembelajaran “Global Open Access Learning System” (G.O.A.L.S) di Universiti Sains Islam Malaysia (USIM). Untuk mengecilkan skop kajian, kakitangan daripada sistem GOALS disasarkan sebagai populasi kajian ini. Risiko keselamatan maklumat GOALS akan diramal dan dikelaskan berdasarkan borang soal selidik berstruktur yang senarai itemnya diperolehi melalui satu kajian menyepadukan keselamatan maklumat dalam persekitaran E-Pembelajaran yang melibatkan tiga perkara mengenai kategori risiko keselamatan maklumat umum iaitu; (1) pembebasan maklumat tanpa kebenaran, (2) pengubahsuaian maklumat tanpa kebenaran, dan (3) penafian penggunaan sumber tanpa kebenaran. Sementara itu, data yang diperolehi daripada responden telah melalui penilaian risiko yang terdiri daripada empat langkah iaitu; (1) Menentukan ancaman keselamatan maklumat, (2) Penilaian risiko, (3) Cadangkan remedi bagi ancaman keselamatan maklumat, dan (4) Mengkaji penilaian. Hasil kajian menunjukkan bahawa ancaman teknologi adalah jenis ancaman keselamatan maklumat yang dihadapi oleh GOALS di USIM. Ia melibatkan gangguan untuk mengakses sistem oleh pensyarah dan pelajar kerana kelajuan jalur lebar yang lemah, masalah server dan sebab-sebab lain. Kemudian, ia juga melibatkan pemintasan kepada sistem yang melumpuhkan atau memutuskan sambungan pensyarah atau pelajar apabila mereka memuat naik atau memuat turun fail dalam sistem, dan juga apabila pelajar menduduki kuiz atau ujian. Kawalan akses menggunakan firewall adalah dicadangkan sebagai remedi bagi ancaman keselamatan maklumat yang dihadapi oleh GOALS di USIM. Firewall merupakan gabungan sistem peralatan dan program keselamatan terjamin untuk mengelakkan akses yang tidak dibenarkan kepada sistem korporat dari luar organisasi.

ABSTRACT

This study investigates the problem of information security risk associated with E-Learning Systems of Global Open Access Learning System (G.O.A.L.S.) in Universiti Sains Islam Malaysia (USIM). To narrow down the scope of the study, staffs from GOALS system are targeted for the population of this study. The information security risks of GOALS will be predicted and classified on a well structured based-questionnaire that was based on items derived from the study integrating information security in an eLearning environment that involves three items on general information security risks categories which are; (1) Unauthorized release of information, (2) Unauthorized modification of information, and (3) Unauthorized denial of resource use. Meanwhile, data obtained from respondents went through risk assessment that consists of four steps that are; (1) Determine information security threats, (2) Risk evaluation, (3) Propose remedies for information security threats, and (4) Review the assessment. Results showed that Technological threats is the type of information security threats faced by GOALS in USIM. It involves 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. Access control using firewall is proposed as remedies for information security threats faced by GOALS in USIM. A firewall is a blend of equipment and programming security system secured to avert unapproved access to a corporate system from outside the organization.

TABLE OF CONTENT

CHAPTER 1: INTRODUCTION

1.1	Introduction	1
1.2	Research Motivation	3
1.3	Background of the Research	3
1.4	Problem Statement	5
1.5	Research Questions	6
1.6	Research Objectives	7
1.7	Scope	7
1.8	Definition of Terms	8
1.8.1	E-learning	8
1.8.2	Information Security	8
1.8.3	Information Security Risks	8
1.8.4	Risk Assessments	9
1.8.5	Risk Analysis	9
1.8.6	Computer Security	9
1.9	Methodology	10
1.10	Limitation of the Research	10
1.11	Summary	11

CHAPTER 2: LITERATURE REVIEW

2.1	Introduction	12
2.2	E-Learning	13
2.2.1	The Development of E-learning.	13
2.2.2	Challenges in E-Learning	14
2.3	E-Learning Security	16

2.3.1	Basic Security Requirements	20
2.3.1.1	Access Control	21
2.3.1.2	Confidentiality	21
2.3.1.3	Integrity	22
2.3.1.4	Availability	23
2.3.1.5	Non-Repudiation	24
2.3.1.6	Authentication	24
2.3.1.7	Privacy	25
2.3.2	E-Learning Vulnerabilities	26
2.3.2.1	User Privacy Vulnerability	26
2.3.2.2	Content Vulnerability	26
2.3.2.3	Web-based Application Vulnerability	27
2.3.3	Risk Assessment in E-Learning	28
2.3.3.1	Security Threat Source	31
2.3.3.2	Security Threat Classification	33
2.3.3.3	Remedies of Risks	36
2.3.3.4	Types of Security Attacks for E-Learning	40
2.3.3.5	Risk Analysis	45
2.3.3.6	Steps for Risk Assessment	45
CHAPTER 3: MATERIALS AND METHODOLOGIES		
3.1	Introduction	47
3.2	Research Design	47
3.2.1	Ethical Overview	48
3.2.2	Accessibility of Information	48
3.3	The Resources	49
3.4	Research Methods	49

3.5	Risk Assessment Methodology	49
3.6	Method of Data Collection	50
3.7	Questionnaire Validation	51

CHAPTER 4: RESEARCH RESULTS

4.1	Introduction	53
4.2	Respondents' Characteristics	53
4.2.1	Gender	54
4.2.2	Education Level	54
4.3	Descriptive Analysis of Questionnaire	54
4.3.1	Unauthorized Release of Information	55
4.3.2	Unauthorized Modification of Information	56
4.3.3	Unauthorized Denial of Resource Use	57
4.4	Risk Assessment	58
4.4.1	Risk Assessment Step 1: Determine Information Security Threats	59
4.4.1.1	Human Threats	59
4.4.1.2	Technology Threats	60
4.4.2	Risk Assessment Step 2: Risk Evaluation	63
4.4.3	Risk Assessment Step 3: Proposed Remedies for Information Security Threats	64
4.4.4	Risk Assessment Step 4: Review the Assessment	65
4.5	Summary	66

CHAPTER 5: DISCUSSION AND CONCLUSION

5.1	Introduction	67
5.2	Discussion	67
5.3	Conclusion	68

5.4	Future Work	69
REFERENCES		70
APPENDICES		
Appendix A	Research Timeline- Milestones	75
Appendix B	Plagiarism Result	76
Appendix C	Questionnaire	77
Appendix D	Certificate of Publication	81
Appendix E	Publication.. (A Review Of Security Threats By The Unauthorized In The E-learning)	82
Appendix F	Brief Biodata	83

LIST OF TABLES

Table 3.1	Questionnaire Validation Table	51
Table 4.1	Gender	54
Table 4.2	Education Level	54
Table 4.3	Descriptive Statistics of Unauthorized Release of Information	55
Table 4.4	Descriptive Statistics of Unauthorized Modification of Information	56
Table 4.5	Descriptive Statistics of Unauthorized Denial of Resource Use	57
Table 4.6	Descriptive Statistics of Human Threats	60
Table 4.7	Descriptive Statistics of Technological Threats	61
Table 4.8	Information Security Threats in GOALS	62
Table 4.9	Risk Evaluation of Information Security Threats in GOALS	63
Table 4.10	Proposed Remedies for Information Security Threats in GOALS	64

LIST OF FIGURES

Figure 2.1	E-Learning Readiness Model (Source: Darab & Montazer, 2011)	14
Figure 2.2	The E-Learning Challenges (Source: Alwi & Fan, 2010)	15
Figure 2.3	Security Modeling of E-Learning (Source: Yong, 2007)	19
Figure 2.4	Relationships in Risk Management (Source: Zhiwiei & Zhongyuan, 2012)	29
Figure 2.5	Organization of Secure (Source: Barik Karforma, 2012)	37