TO PROPOSE THE COMPREHENSIVE UNIVERSITY FRAMEWORK FOR SECURE INFORMATION SYSTEMS

ABDULRHMAN AHMED ABDULRAZAQ

MASTERS OF SCIENCE

AL-MADINAH INTERNATIONAL UNIVERSITY

MAY 2014 / 1435H

A Comprehensive University Is Security (UISS) Framework For The Protection Of Universities Information Systems

ABDULRHMAN AHMED ABDULRAZAQ

Thesis Submitted to
Computer Sciences Al-Madinah International University in Fulfillment of the Requirements for the Degree of MASTERS OF SCIENCE

MAY 2014

صفحة التحكيم

CERTIFICATION OF DISSERTATION WORK PAGE

أُقرَّ بحث الطالب عبدالرحمن أحمد عبدالرزاق بعنوان *A Comprehensive Data Security Model for the Protection of Al Yamamah University Information Systems* من قِبل الآتية أسماؤهم:

The thesis of student named: ABDULRHMAN AHMED ABDULRAZAQ under title *A Comprehensive University Is Security (Uiss) Framework for the Protection of Universities Information Systems* has been approved by the following:

المشرف على الرسالة Academic Supervisor

.....	**الاسم /Name**
.....	**التوقيع/Signature**

المشرف على التصحيح Supervisor of correction

.....	**الاسم /Name**
.....	**التوقيع/Signature**

رئيس القسم Head of Department

.....	**الاسم /Name**
.....	**التوقيع/Signature**

عميد الكلية Dean, of the Faculty

.....	**الاسم /Name**
.....	**التوقيع/Signature**

قسم الإدارة العلمية والتخرج Academic Managements & Graduation Dept

عمادة الدراسات العليا Deanship of Postgraduate Studies

DECLARATION

I hereby declare that, this dissertation is the result of my own investigation, except where otherwise stated.

Name: **Abdulrhman Ahmed Abdulrazaq**

Signature ……

Date: ……...

PERMISSION TO USE

In presenting this thesis in fulfillment of the requirements for a postgraduate degree from Al-Madinah International University, I agree that the University Library make it freely available for inspection. I further agree that permission for copying of this dissertation in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor or, in his absence by the Dean of Faculty of Finance & Administrative Sciences or the dean of Postgraduate Studies. It is understood that any copying, publication, or use of this dissertation or parts thereof for financial gain shall be given to me and to Al-Madinah International University for any scholarly use which may be made of any material from my dissertation.

Request for permission to copy, make other use of materials in this thesis, in whole, or in part should be addressed to:

Dean of Faculty Computer Sciences or the dean of Postgraduate Studies

40100
11th Floor –Plaza Masalam
Sec 9, Shah Alam
Malaysia

ABSTRACT

In this study, an analysis of data security of the university information systems is performed and then a data security model has been proposed in order to address the identified concerns. Authenticity and integrity of university data is quite vital not only for the universities but also for the society overall because any discrepancy in the university data especially in the exam data will result in bringing the corrupt and dishonest people at the higher positions. Keeping in view the high importance of security of university data, this study proposed a Lattice model which will make the university information systems to be much more secure.

The study, first of all, identified the genuine security issues of such systems by observing the information system of one university and analyzing the literature. This study has adopted methodological triangulation type sampling in which a combination of sampling methods can be used in the data collection process. The instruments mainly used for the data collection were surveys and interviews. Five universities from Saudi Arabia including Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University were selected for the purpose of this data collection. A total number of 158 respondents from five universities participated in this survey. A number of critical security breaches have been identified with this process, which were imposing a great question mark on the integrity of the data.

In order to address the identified concerns, the study further developed a security model which addressed all the identified concerns and if used properly, this can serve as a tool of great assistance for the security of university information systems. In addition University IS Security (UISS) Framework was proposed based on the survey results to prevent security threats in universities information systems. Cloud/network security, system security and web security SQL injection were recommended and included in the proposed framework. The proposed model includes authentication and authorization mechanism designed specifically for all five universities. To ensure consistent data access across all levels of the conceptual model, the mechanism relies on robust query re-writing

rules. The proposed model has in-flow communication mechanism which prevents complicated inferences using the initial query restrictions along with removing the remaining inferences. The proposed model is based on object-oriented security design that collectively produce a useable infrastructure.

ACKNOWLEDGEMENT

I would like to express my gratitude and appreciation to supervisor whose untiring efforts and support gave me great strength and power to deal with the complexities of this research. He took my hand at every step and guided me through every challenge that came on my way. I will never forget his support and I am sure this learning process will be a great asset for me throughout my life.

Thank you very much.
Abdulrhman Ahmed Abdulrazaq

DEDICATION

I dedicate this dissertation to my parents who provided me unconditional support and courage during the course of this research. Their support enabled me to progress through all the stages of this research with confidence. I am sure that successful completion of this research will give them a great satisfaction. I will, also, never forget these challenging moments along with the companionship of my parents.

TABLE OF CONTENT

CERTIFICATION OF DISSERTATION WORK PAGE III
DECLARATION IV
PERMISSION TO USE V
ABSTRACT VI
ACKNOWLEDGEMENT VIII
DEDICATION IX
TABLE OF CONTENT X
LIST OF TABLES XII
LIST OF FIGURES XIV
LIST OF ABBREVIATIONS XV
CHAPTER 1 - INTRODUCTION 1
1.1. Background 1
1.2. Thesis Problem 2
1.3. Research Questions 4
1.4. Thesis Objectives 4
1.5. Scope of Study 4
1.6. Thesis Plan 5
CHAPTER 2 - LITERATURE REVIEW 7
2.1. Introduction 7
2.2. Information Systems for Business Organizations 8
2.3. Security Concerns Related to the Business Information Systems 9
2.4. Educational Information Systems 11
2.5. Information Security Concerns Related to Educational Information Systems 11
2.6. Cloud/Network Security 16
2.7. Web Security SQL Injection 17
2.8. Security Risk in University Network 17
CHAPTER 3 - RESEARCH METHODOLOGY 18
3.1. Introduction 18
3.2. Research Design 18
3.3. Research Method 19
3.4. Instruments of data collection 20
3.5. Ethical Issues relevant to the study 21
3.6. Universities 23

3.7. The Proposed Model 23
CHAPTER 4 - DATA ANALYSIS & DISCUSSION 29
4.1. Introduction 29
4.2. Main Characteristics of the Samples 29
4.3. Security and Responsibilities in All Five Universities 30
4.3.1. Information Security Awareness *31*
4.3.2. The responsible of Information Security *32*
4.4. Security Threats in the Universities 34
4.4.1. Handling the information *35*
4.4.2. Computer Usage *38*
4.5. Improving Security 39
4.5.1. Cloud/Network Security *40*
4.5.2. System Security *42*
4.5.3. Web Security SQL Injection *44*
4.6. Comparison between Five Universities 46
4.7. Discussion 54
4.8. Summary 57
CHAPTER 5 - FINDINGS AND CONCLUSIONS 59
5.1. Introduction 59
5.2. Strengths and Weaknesses of the Model 59
5.2.1. Strengths *59*
5.2.2. Weaknesses *61*
5.3. Contribution of this study 61
5.4. Future Work 62
5.5. Conclusion 62
REFERENCES 65
APPENDIX (A) 68

LIST OF TABLES

Table 2.1: IS security concerns as mentioned in the literature 14

Table 4.1: Proportions of men and women in the study sample 29

Table 4.2: Distribution of the sample respondents within the age groups 30

Table 4.3: Distribution of employees' role in AL Yamamah university 30

Table 4.4: Information security awareness 31

Table 4.5: Distribution of the sample respondents according to responsible party of IS 32

Table 4.6: Received training on information security awareness 33

Table 4.7: Understanding of policy and regulation of using the facilities 33

Table 4.8: Distribution of information type involved in the participants' work 34

Table 4.9: You are asked to provide information containing names and contact details to another office. What is an appropriate method for sending this information? 35

Table 4.10: Handling sensitive information 36

Table 4.11: Individuals protecting their computers and data 36

Table 4.12: Remotely accessing the university shared drives, files, applications and emails 37

Table 4.13: Important information that would be of interest or values to others 37

Table 4.14: Sharing login and passwords with the team 38

Table 4.15: Providing password to a known collogue 38

Table 4.16: If someone e-mails you an attachment/link that is not work related, how likely are you to open it? 39

Table 4.17: Cloud/Network Security 1 40

Table 4.18: Cloud/Network Security 2 41

Table 4.19: System Security 43

Table 4.20: Web Security SQL Injection 45

Table 4.21: Gender Comparison Among Five Universities 47

Table 4.22: Security and Responsibilities in Five Universities 48

Table 4.23: Individuals protecting their computers and data 48

Table 4.24: Cloud/Network Security 50

Table 4.25: System Security 51

Table 4.26: Web Security SQL Injection 53

LIST OF FIGURES

Figure 3.1: The Proposed Model for University 24

Figure 3.2: The Proposed University IS Security (UISS) Framework 28

LIST OF ABBREVIATIONS

D&M	Delone and McLean
ERP	Enterprise Resource Planning
Ecar	Educause Center for Analysis and Research
ICT	Information and Communication Technology
IS	Information System
VPN	Virtual Private Network

Chapter 1 - INTRODUCTION

1.1. Background

Educational institutions have an abundant information and data produced within the different sections and with the interdepartmental communication. Various educational and non-academic departments produce a great deal of data each day that is important in nature and carries great value not just for the university, management and teaching staff but additionally for the students. It is relatively necessary to guarantee the credibility and reliability of the university data to ensure that mistake free and genuine transactions could be processed.

To be able to arrange university data and to carry out smooth transactions depending on this data, universities are actually shifting in the direction of the deployment of information system solutions which incorporate the routines of all the academic and non-academic departments at one central place. This guarantees the data persistence and credibility. The data offered with the information systems is not superfluous and simple data entered at one location is available to all the appropriate places. For example, various departments like management, researchers, enrollment and exam don't have to get into the basic students' data. Instead this information is once entered in the information system by registration department and then it is automatically accessible to the rest of the appropriate departments. Additionally, departments may view and utilize the information but are not able to add, modify or erase the basic data of students. In the similar way, all other departments carry out their features by adding, upgrading and removing the data related to their department and then making this information accessible to the other departments to be utilized for their own needs. This will save a great deal of effort, provides precision and persistence within data and guarantees the smooth data transactions.

But there are some serious concerns which have arisen with the utilization of latest data processing approaches, both from the critics of information systems and from the supporters of these systems. These concerns are mainly related to the data security.

According to this common perception, university data is now more vulnerable than it was ever. Introduction of information system has introduced the fast and consistent processing of data but it has become an easy target for the ones who want to use these systems for their own personal benefits. Now anyone with a destructive frame of mind may attempt an intrusion within the educational information system and add, update and delete the data in an undesired way. According to (Furnell & Karweni, 2001), in a survey conducted by security community, an archive of hacked website was developed which included 20 Universities.

Data available with different departments of the universities is of quite critical nature for example records of fees and dues, examination scores records, inventory, HR, finance, academics and administration, all pieces of data hold a great worth for the organization and organization cannot afford to compromise the integrity of data which may otherwise result in severe consequences for the organization.

Keeping in view the importance of data and questions arisen over the data available with the university information systems, higher management of the universities are now in need of a fool proof mechanism to ensure that data available with their information system is secure and is not being used in a wrong way. This study is an attempt to analyze this issue, understand any potential threats to the university data and come up with a comprehensive information security model which can guarantee that data is secure and has not been utilized for any ulterior purpose. Findings of this study will be quite vital for all the related segments including higher university management, university administrators, management, staff, and faculty and also for the students. It will act as a protection model above the existing information systems. Furthermore, some options related to cloud/network security, system security and web security SQL injection are suggested by this study to protect university network.

1.2. Thesis Problem

University Information Systems normally face severe data security concerns and their data is not safe from unauthorized usage. This study has aimed to address the security information system based on existing framework. Universities are the source of

growth for a nation. The individuals having gone through the educational process within the university serve as the backbone of the nation. If universities become a place of corruption and start producing the generations which are not desired, can be a big blow for a nation. Normally universities data, especially results data, is not secure and unauthorized people get access to the data and are even able to modify it for the wrong purposes. Universities information systems are at great risk in the matter of data security (Yang, Lin, & Lin, 2002). Higher education data has critical breaches with respect to technical implementation of security measures (Oblinger, 2003). This is normally because of lack of appropriate planning at the ERP planning stage (Alfawaz, May, & Mohanak, 2008) and the access control techniques in traditional data management system cannot be directly applied to universities. Specifically, Universities' conceptual data model is considerably more abstract than the relational models used by conventional relational database management systems. In addition, the current access control methods are more vulnerable to subtle inferences attack This may result in serious consequences for a university. If data is not utilized properly, it will cause the creation of a society which is morally corrupt, resulting in overall social degradation.

Cloud system is affected by the threats and attacks directly or indirectly. Cloud security is used to prevent or respond to security threats. Many cloud providers used some network security solutions and techniques such as Firewalls, Intrusion Detection Systems (IDS), and Anti-Virus Gateway to protect end-systems from attacks. A type of injection or attack in a Web application is called SQL Injection. In this kind of injection, in order to gain unauthorized and unlimited access the attacker provides Structured Query Language (SQL) code to a user input box of a Web form. Injecting a Web application is like having access to the data stored in the database. An unauthorized access to this data can threat the confidentiality, integrity, and authority as this data could be confidential and of high value like the financial secret of a bank (Kindy & Pathan, 2011). One of the most important assets of each university is information that must be protected from security breach. Thus, security threats in university networks must be controlled to reduce the risk of security breach. University must provide secure access to the users and defend them from vulnerabilities and security breaches. Identification and assessment of critical threats is required in university campus network to reduce security dangers.

1.3. Research Questions

This research seeks to find out answer to the following main research question: “How can we improve the level of information security in university information systems?”

In order to answer this main question, this study will seek answers to the following questions:

- What are the genuine threats related to the security of universities’ information systems data?
- What are the reasons of security threats?
- How can we overcome to identified data security risks and make educational information systems more secure?

1.4. Thesis Objectives

The research aims to address the issues of the information security in among information systems in five universities including Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University in Saudi Arabia to secure such systems from possible vulnerabilities through the following objectives:

- To identify the threats that may arise within university information systems.
- To study the reasons of universities’ security threats by using the qualitative survey and interview.
- To propose model based on existing security framework that can provide access and inference control to secure the university’s information system from possible vulnerabilities, which has been addressed by the surveys and interviews, and at the same time perform a reliable transaction.

1.5. Scope of Study

In this study, we have developed a comprehensive information security framework for educational information systems. Scope of my study will be limited to the following:

- The study found potential security issues with the help of surveys, interviews with students, teachers, staff, higher management and a data security expert.
- Data was collected from five universities comprising Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University in Saudi Arabia.
- Data related to different departments of the universities was looked for any security breaches. These departments include Registration, HR, Exam, Faculties and Finance.

1.6. Thesis Plan

This chapter has introduced the research with a detailed background description. Then the thesis problem was elaborated and based on the problem, thesis objectives are defined in the subsequent section. This led to the development of our research questions. At the end of the chapter scope of this study has been described.

Chapter No 2 is the chapter of literature review which describes the different dimensions of the literature related to our topic. Initially literature review related to information systems for business organizations in general were discussed. Then security concerns related to business information systems are discussed. Then a detailed description of educational information systems and their security concerns are discussed in detail.

Chapter 3 describes the Research methodology. Sections of this chapter include research design, research method, instruments of data collection, ethical issues related to study and a description of selected university.

Chapter 4 of this report provides data analysis based on the research conducted and comparison between the collected data from five universities.

The final chapter of Findings and Conclusions summarizes the findings of this study by proposing a security model, describing the contributions of this study, future work and conclusions.

Chapter 2 - LITERATURE REVIEW

2.1. Introduction

Even when there were no computers and technology application in the business information security and risk prevention was considered to be one of the basic process. Now when the businesses are more dependent on the technology based information system the requirement of the security has increased. For the existence and the prosperity of the business it is essential to safe guard and protects the business information. It is necessary for any business to ensure reliable and secure information transaction for the smooth running of the business process.

Information system security is a challenging in today's world. The challenges on this filed include computer crime, data privacy, copyright, etc. It is dynamic in nature with ever changing need and demands. It has to be addressed with agility and promptly. With the innovation in technology there are different kind of vulnerabilities and challenges faced by the information system security (Anonymous, 2003).

Apart from the technology changes the global market is also rapidly changing. The trends come and go very quickly. To meet up with the market changes it becomes essential to apply the required modification in the information system without testing and proper checks. This mostly results in security laps and risks.

There are two important goals of any business who want to minimize the risk of information security breach. First, it is essential to identify the risk associated with the information system security. And second, by overcoming those risks increase the efficiency of the information system (Angell & Smithson, 1991). Whereas "effectiveness is doing the right things" (Nanda, 2008). In order to minimize the risk to the information system and to increase the efficiency of the system it is necessary to understand how technical and non-technical security measures interact and influence each other. The information system acts as a balance between the culture, methods and machines (Nanda, 2008).

2.2. Information Systems for Business Organizations

The importance of the information system is critical for any business in today's world. Every business small or large is dependent on the Information technology for the existence and prosperity of the business. Information system is not limited to the physical or the technological in an organization. In fact, it is the representative of the attitudes, culture and behaviors of the business (Jones, 1979). The potential of the business to prosper and become successful is dependent on its ability to organize and maintain information. Information system thus hold and essential and purposeful position in any business (Avgerou & Cornford, 1998). "The complex interplay of the formal and the informal systems in an organization gives rise to the management systems that are in place. The advances in new technology and the emergent organizational forms introduce new capabilities and 'connectivity' for information processing" (Jones, 1979). A lot of work is available in the literature, discussing different dimensions of information systems some of which are as follows.

- The study (Bernroider, 2008) has empirically analyzed the success ratio of efforts involved with organizational Enterprise Resource Planning (ERP) system development. The study has thrown light on the alignment of ERP strategy, commitment of stakeholders and team development strategies etc. Popular Delone and McLean (D&M) IS success model was taken up for this purpose. The study developed certain questions to observe existing practices. The study concludes that an efficient mechanism of IT control enhances success ratio.
- The study (Petter, DeLone, & McLean, 2008) reviewed 180 research papers, related to the Information Systems, over the span of 15 years. These papers dealt with the aspects of IS success. The study analyzed six dimensions of DeLone and McLean (D&M) model. This work has been established on the prior studies and summarized the measures of Information Security (IS) success. According to the results of this study, over the years only a little progress has been observed in the measurement procedures of information systems. Researchers still take into

account a limited amount of dimensions to observe its performance rather than following a comprehensive approach. As a result, a clear scenario cannot be developed to measure the performance of Information Systems. The study has emphasized on the development of comprehensive approaches of measuring IS success.

- An investigation of resistance to the information system security has been discussed in the study (Kim & Kankanhalli, 2009). This study has highlighted the resistance that a new IS receives from the stakeholders, before its implementation. It also provides recommendations to the management to overcome this resistance. Based on the previous research, this study develops a theoretical model by synthesizing user resistance and technology acceptance theories. According to this study, switching cost is the main reason of user resistance. The study also identifies the perceived level of IS change and support from the organization as the influential factors in this regard.
- (Khajaria & Kumar, 2011; Krishnan, 2013; Kumar, Gosain, & Singh, 2010, 2014) propose security models that restrict data warehouse access. Some of them focus on the design process for example; one approach allows multi-dimensional security constraints. Other have developed have proposed security requirements for the entire life cycle of the data warehouse. (Khajaria & Kumar, 2011) Propose agent goal decision information model for the development of data warehouse that support the early and requirement.
- (Altamimi & Eavis, 2012; Kabra, Ramamurthy, & Sudarshan, 2006; Liu, Zhang, Chen, & Wang, 2014; Zhang, Wang, & Khan, 2015) focus on developing traditional data managements systems with expressive security policies and access control systems (access control mechanisms).

2.3. Security Concerns Related to the Business Information Systems

The world has changes immensely and is rapidly changing into a global market. Like the needs and the demands of the business world is changing similarly the requirements of the IT world is changing with the same pace and momentum. Now a day

new and more serious challenges are faced by the information system securities. The vulnerabilities have increased with critical impacts (Stojaković-Čelustka, 1998). After having gone through some studies related to the information systems in general, we will now have a look at some work on the security of information systems.

- The application of Information Security policies in UK based organizations have been analyzed in (Fulford & Doherty, 2003). This study has attempted to explore the success factors which are critical for the implementation of information system security in an organization. This has been done from the expert's perspective. The study has mainly focused on the topic with respect to the implementation of security procedures in the government organizations. The methodology of the study is exploratory with a qualitative approach for collecting and analyzing the data. The study suggests that business organizations must develop such policies which can serve as a tool of protection against undesired access to their resources. Appropriate trainings for employees must also be conducted to ensure that they know the best security practices and also the consequences of data insecurity. Top management has been emphasized to exhibit more responsible attitude towards IS security policies which will serve as an example for the lower categories of employees. Moreover, allocation of sufficient budget to ensure IS security is considered as one of the most important considerations. The factors identified in this study are interlinked and we cannot prioritize these factors with respect to their importance.
- The study (Kwahk & Lee, 2008) has examined the role of readiness for change in ERP implementation. It has also highlighted the perceived impact on the ERP system. A model for readiness of change is also developed. Then this model was tested using the data collected from the ERP system in Korea. The study has discovered that readiness for change has a great impact on the successful implementation of ERP system. Readiness for change can be enhanced by the factors of organizational commitment and perceived personal competence. Moreover (Schniederjans & Yadav, 2013) presents critical success factors in ERP

implementation and argues the impact that trust with the vendor, system and consultant has on ERP implementation success.

2.4. Educational Information Systems

Now we will have a look at some studies related to the entity of our research i.e. educational information systems. A lot of work is available discussing different dimensions of educational ERP or information systems. Here, we will discuss a few very important studies.

The study (Bologa, Muntean, Sabau, & Scorta, 2009) has evaluated some other important studies regarding the implementation of ERP systems in business organizations and analyzed them with respect to the Romanian universities. Critical success factors have been observed and their differences are measured with respect to ERP implementation in the universities. The study suggests that special attention must be given to the human factors. The outcomes of this study were to be used for the development of ER framework for universities and it had to be tested against a Romanian university. Some important differences with regard to the structure of communication, management participation, organization, capabilities of implementation team, communication procedures, training of users and etc. were observed. Some other studies focused on the critical factors of EPR systems in higher education such as (Aljohani, Peng, & Nunes, 2015; Olugbara, Kalema, & Kekwaletswe, 2014).

2.5. Information Security Concerns Related to Educational Information Systems

Now, the existing literature related to security in educational information systems will be discussed in detail.

- Information security elements which are necessary for e-learning environments have been discussed in detail in (Alwi & Fan, 2010). The study also discusses the current situation and the available literature on the topic. Moreover, the study seeks to reduce information security risks in e-learning environment. According to

the study, it is quite necessary to take strict security measures related to the hardware and software for the integrity and reliability of the data.

- Educause Center for Applied Research (ECAR) study of IT security (Kvavik & Voloudakis, 2003) has analyzed the security procedures in the sector of higher education which is normally considered to be an open environment rather than too tight with respect to the security of data. The study has emphasized over the need to invest on hiring good security experts as absence of any information security procedures results in severe consequences and a sense of insecurity for the organization. People behavior also plays an important role in the successful implementation of security policies whereas an irresponsible behavior may result in the intrusion into the system with the help of viruses, worms and super worms.
- The study in (Alfawaz, May, & Mohannak, 2008) proposed a security practitioner's management model to secure information systems of universities. The model has also considered the actual implementation of security procedures throughout the organization introducing a culture of compliance in this educational sector. According to this study, normally information security procedures are undertaken at the extreme end of system development and deployment which is not a good approach. This can provide the implementation of security up to a specific level but security cannot be guaranteed. The study also pointed out that normally ensuring of security implementation is the responsibility of operational officers and kept isolated from the other factors of the university. The study suggests that a strong security model must be developed during the ERP planning and human resources up to all levels must be kept responsible for the implementation of security procedures. In addition, (Alsultanny, 2014) enhance the computer network security and to protect the computer network.
- The study in (Bhilare, 2013; Oblinger, 2003) has highlighted the importance of development of security procedures in the educational organizations with respect to the mission of higher education, values, physical environment and security practices. The study has greatly emphasized on the implementation of values which include community, anatomy, privacy and fairness. Firewalls, VPN content

filtering, logging, packet filtering and intrusion detection have been considered as some of important practices in this regard.

- The study in (Yang, Lin, & Lin, 2002) has presented an information security scheme for collaborative e-education systems. Privacy and security are very important elements in education systems. This study has designed certain policies and security procedures to be used in e-learning systems.
- The issue of information system security in online learning system has been undertaken in (Chen & He, 2013; Furnell & Karweni, 2001). According to the study, security is usually not taken as an important element in the development of educational systems. The study has emphasized over the need for developing sound security procedures and presented important security requirements and main technical aspects. It has stressed over the need to utilize strong authentication and access control and like any other business systems of important nature, educational systems have no immunity in this regard.
- The privacy concerns that organization rely upon to control abstraction have been addressed in (Dia & Farkas, 2015; Gollmann, 2010; Jahid, Gunter, Hoque, & Okhravi, 2011). Those abstractions are mechanisms and security policy which they are high-level requirements determine who to access the specific data and under what circumstances. The study has defined a series of conditions such as restrictions and exceptions to be set by the administrator to control users access and at the same time provide monitoring their access. The responsibility of the security mechanisms is to impose security policies, it translates and evaluates a user's access request against the defined security policy.

There are great concerns about the integrity and reliability of data available with the university information systems. Universities have implemented information systems with great functionality and ease of use for transactions processing but still lack appropriate security measures. This has undermined the real worth of information systems and all the related entities within the educational systems are in doubt about whether they are gaining the desired benefits of these information systems or these are

merely serving as a tool of victimization by certain segments. We can find evidence about this perception of data security from the literature as follows:

- According to (Amoako-Gyampah & Salam, 2004; Tsai, Compeau), implementation of information systems is risky with respect to data security because it requires organization wide initiatives and organizations are slow to adopt these.
- Educational institutions are adopting ICT without any appropriate planning and understanding of any relevant security concerns (Alwi & Fan, 2010; Kambourakis, 2013).
- Universities fail to deploy security procedures during the development of educational information systems which is quite difficult for them to adopt at later stages (Alfawaz et al., 2008).
- Colleges and universities face a number of security vulnerabilities, ranging from network resources to students owned equipment (Oblinger, 2003).
- There is an increasing data abuse with the arrival of information systems (Chen & He, 2013; Furnell & Karweni, 2001).

The following table synthesis the concerns related to information systems security in the universities, as mentioned in the literature.

Table 2.1: IS security concerns as mentioned in the literature

Study	**IS Security Concern**
(Alwi & Fan, 2010; Kambourakis, 2013)	E-Learning systems are exposed to illegal internet activities
(Kvavik & Voloudakis, 2003)	The higher education information systems data is at the risk of viruses, worms and super worms and causes a great sense of insecurity for the organization

(Alfawaz et al., 2008)	Universities' data is not secure because normally information security procedures are undertaken at the extreme end of system development and deployment which is not a good approach and this is also a problem that normally security responsibility is kept limited to the operational officers and other actors not considered
(Oblinger, 2003)	While devising the Higher education security policies, the higher education mission and values are not considered. At the same time, critical technical implementations like Firewalls, VPN content filtering, logging, packet filtering and intrusion detection are also overlooked.
(Yang et al., 2002)	Collaborative education systems and e-learning systems are at a greater risk with respect to data security.
(Chen & He, 2013; Furnell & Karweni, 2001)	Security is usually not taken as an important element in the development of educational systems. There is an increasing data abuse with such systems
(Amoako-Gyampah & Salam, 2004)	Implementation of information systems is risky with respect to data security because it requires organization wide initiatives and universities are slow to adopt these
(Alwi & Fan, 2010)	Educational institutions are not implementing the ICT with proper planning and analysis

In this section, previous related work has been discussed in detail, starting with the work related to information systems in general, then security implementation in information systems, then educational information system followed by educational information systems security. This has presented a comprehensive picture of what has already been done and what is missing in the literature. A reasonable amount of work is available on educational information system, especially on e-learning aspect of it. We did not find much work focusing on security requirements specific to the educational information systems. Some work on security which is available has focused on the e-learning aspect of educational systems rather than the complete management information

system and so we are missing with any proposed security model, specifically developed for educational information systems. This study has proposed to fill this gap in the literature.

There are three main parts of the Sensitive information systems. First, the communication Channel second is the user interface and last is the sensitive information storage. The surveillance of these three parts sums to the protection of sensitive information itself. In order to minimize the risk associated with the information system security it is essential to take these components into account. If any one component is neglected it may result in affecting the efficiency of the information system. This has multiple effects on the business in terms of trust, knowledge and performance.

There is no total security solution exists to help protect sensitive information in the three components. Issues such as dynamic sensitive information ownership, group authentication and authorization and privacy protection give raise to some problems that needs to be addressed for the protection of sensitive information systems (Nanda, 2005).

2.6. Cloud/Network Security

On demand services over the Internet are offered by cloud computing using virtual storage with less computing infrastructures and cost of services. These security services are granted to individuals and organizations to transfer their application, data and services to the cloud storage server. Security services are provided by the trusted third party through the Internet and uses many web technologies that evolve new security issues. Therefore, cloud security is required to set policies, technology, and control that are helpful data and services protection. Cloud system is affected by the threats and attacks directly or indirectly. Cloud security is used to prevent or respond to security threats. Many cloud providers used some network security solutions and techniques such as Firewalls, Intrusion Detection Systems (IDS), and Anti-Virus Gateway to protect end-systems from attacks. In addition Intrusion Prevention Systems (IPS) is used to gain high level security and performance in networks (Modi et al., 2013). Finally, implementing secure backup and recovery process allows cloud providers to meet disaster recovery and to prevent accidental or malicious data deletion.

2.7. Web Security SQL Injection

Structured Query Language (SQL) is considered as high level language used in various relational Database Management Systems (DBMS). A type of injection or attack in a Web application is called SQL Injection. In this kind of injection, in order to gain unauthorized and unlimited access the attacker provides Structured Query Language (SQL) code to a user input box of a Web form. Injecting a Web application is like having access to the data stored in the database. An unauthorized access to this data can threat the confidentiality, integrity, and authority as this data could be confidential and of high value like the financial secret of a bank. Therefore, the system in companies or organizations such as bank, university etc. could bear heavy loss in giving proper services to its users or it may face complete destruction. The attack may acquire the confidential and private information and endanger the reputation of that organization (Kindy & Pathan, 2011). Consequently, SQL Injection could be very risky for reputable organizations such as universities.

2.8. Security Risk in University Network

Information security became an essential element in business management and they must improve information security level. Government set regulations and standards to protect information assets in organizations because of the increasing threats and cost of security failure. Advancement of information technology and the need of network applications in universities environments result vulnerable computing environment with more security threats. Universities are competing to be some of the most technologically advanced places in the world by offering facilities such as Wi-Fi support, online learning using lecture capture software, digital library, classroom virtualization, web conferencing etc. One of the most important assets of each university is information that must be protected from security breach. Thus, security threats in university networks must be controlled to reduce the risk of security breach. University must provide secure access to the users and defend them from vulnerabilities and security breaches. Identification and assessment of critical threats is required in university campus network to reduce security dangers.

Chapter 3 - RESEARCH METHODOLOGY

3.1. Introduction

The issue under consideration is not only important; in fact, it is critical for any educational institute. Universities are responsible for the present and the future of the nation. They have heavy burden and huge responsibility on their shoulders. The students graduating from these universities form the future of any nation. If the universities lack in producing the desired output this can affect the nation. Data processing and collection is one of the essential processes in any university. Its importance is vital and in case of any disagreement and discrepancy can have serious impacts and consequences. It needs focus, care and proper processing to derive the desired results from data processing.

In this study, we will highlight the issues related to information system security in the university. The obstacles and problem that have the potential to hurdle the performance of the information security system needs to be identified. The main goal of the research is to develop a model to make sure that the university information system is secure and reliable.

The selection of university was based on the type and application of the information security system applied in the universities. The other reason that was considered while selecting the university was the level of the dependence on the information system and the type of data available.

In this study, the level of information security in educational information system in one selected university was analyzed. For this both implicit and explicit data was collected for this system. I conducted surveys, interviews with administration, faculty, students, higher management and data security expert. After identifying the levels of security issues that such systems may have, the next step was to identify the likely factors causing these issues.

3.2. Research Design

This study was to develop a comprehensive security model for educational information systems at the end. Research design that was selected by the researcher is a combination of the descriptive or qualitative research method. There are certain elements and dimensions of the research that cannot be quantified. Even if they are quantified they cannot be accurately interpreted in numeric terms. For a research, statistical tests are used to assess the significance of the observed numeric results, but there are some major concerns for example there are many social aspects of the research which cannot be quantified into numbers and even if they are quantified, the real meanings of the process are lost.

These concerns have led us to the development of qualitative data analysis approaches. Qualitative research explores attitudes and behavior. This is why we got the in-depth and detailed feedback and opinions which helped us in multiple ways throughout our research. Qualitative analysis is a process of information securing, concept building and understanding through uncovering themes with the help of raw data in seeking answer for distinct research questions (O'Leary 2004). Qualitative research has four main methods that are used for the collection of data (Marshal, Rossman, 1998)

- Becoming a part of the environment
- Observation
- Interviews and feedback
- Analysis material collected

Qualitative research explores the attitudes, behavior and experiences of the population of a study. It attempts to get an in-depth opinion from participants. Fewer individuals are a part of the study, but contact with these people lasts longer.

3.3. Research Method

This study performs qualitative analysis in order to explore the research questions. The selection of the university is done with particular care, emphasizing on the application of the information system in comparison to the needs and demands of the

information security system. In our research, multiple sources and techniques are applied in the data gathering process. Using this method, the researcher determines in advance what evidence to gather and what analysis techniques to use with the observations to answer the research questions.

Here an important aspect was to make sure that correct and reflective sample should be considered. To make this possible we have used the methodological triangulation type sampling which is a make up for smaller sample size. According to this type a combination of sampling methods can be used in the data collection process. It not only helps in understand the scenario, but also increases the confidence of the researcher as he can confirm the credibility of the finding from multiple sources. If only one method is used for data collection the researcher can never be confident on the transparency and accuracy of the results and the ambiguity of the research affect the overall performance of the researcher. Researcher is much more confident about the validity of analysis and conclusions of research with triangulation method. For our research the following combination is applied. Data gathered is normally largely qualitative, but it may also be quantitative.

3.4. Instruments of data collection

This is one of the most sensitive, crucial and time consuming part of the research. To make sure the credibility of the research conclusion it is necessary that the data collected should be exact and truly reflecting the current situation. This is why special emphasis is required at this stage. The researcher insured that the data should be collected with care and should be logical. Tools and sources that are used to collect data include

- Surveys
- Interviews

Surveys and Interviews

For this study, data is collected in multiple ways including surveys and interviews. Interviews are conducted with students. In order to have an understanding of

likely issues of educational information systems security it was necessary to have the opinion from all the users of the system. This helped us understand the needs, requirements of an educational information systems security model. The interview was conducted with the help of a semi structured questionnaire.

The questionnaire was designed to seek all the desired information with the help of short, understandable and easy to answer questions. The length of the questionnaire was kept short. The interviewees were divided into two groups. The first group included students. The data collected with the help of the interviews with the first group constituted our primary interview data. The secondary interview data was collected with the help of the interview of the second group that included management and data security experts. Apart from the interviews we have also conducted the focus group discussion. This has helped us understand the user concept and concerns of the information security. Taking views of these people is very important in answering our research questions because they play the key role in this scenario. Surveys were conducted from as many respondents from selected university as possible. Interviews were conducted with the following:

the one hundred and fifty eight 158 students and employees from five universities comprising Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University

Based on the analysis of earlier studies, the number of respondents of interviews is enough to get the opinions of each type of stakeholders. This is a qualitative research which does not need too many participants. Therefore only a few people have been selected for this study. In order to introduce the variety of participants in the study, we have selected participants from different segments. The selected university is from the Saudi Arabia. The universities are selected on the basis of the application and use of the information security system. The analysis of data was performed at the end, based on data collected with the help of interviews and observations.

3.5. Ethical Issues relevant to the study

Each social unit has its own specific social and cultural norms and a researcher must consider and respect these norms while conducting the research. This study followed the strict ethical standards to ensure the protection and confidentiality of responses of participants. It is important to consider that ethical research is in the field of education. It should be considered and respected by all means. It includes the respect and recognition of the privacy of students. Conducting the research keeping it according to the ethical standards will enhance its acceptability and credibility. Place of research, participants and sample size is 158 students and employees from five universities in Saudi Arabia.

The first and most important landmark in the research process was to acquire the permission of the required process from the selected university. A letter of consent was written to the university administration. In the letter the permission for studying and analyzing the information system and its security was requested. With that a pledge of recognizing and following the secrecy requirement of the university was made. After the permission was granted the process of the survey was indicated. The survey was conducted by performing interviews and surveys and in some cases observations. The interview was from students. The sample was taken in small number, for example 158 students and employees from five different universities. The time to complete the on-ground research was limited; still the researcher tried his best to complete the research with utmost accuracy and perfection. This was no doubt the most demanding part of the research and it was full filled with complete dedication and attention. The data collected was then processed and analyzed forming the foundation of the conclusion.

A comprehensive educational information systems security model will be developed based on this analysis of data, considering every possibility. Primary research consisting of the outcomes of interviews and focus group data was compared with the secondary research of literature review. A thorough analysis of each finding will be discussed. Discussion and analysis was completed after consultation with university' higher management and data security experts and then incorporated in the last form.

3.6. Universities

For this study, five universities (Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University) were selected on the basis of the use of information system and the requirements of the security for the said information system. This was a crucial decision as the research and its conclusion were dependent on the right choice.

3.7. The Proposed Model

The information system of a university must cover every single activity of the university and there must be a proper check and balance for each activity. The existing Information Systems of the universities are providing support for the following as shown in Figure 3.1:

- Admissions
- Registration
- Exam
- Finance
- Inventory
- HR
- Library
- Miscellaneous

The system needs to implement a separate module for each of these categories and the module must be completely independent in the functioning. The rights of each module must be assigned to the respective department users only and there must be no overlap of permissions among the users of the system. Every module needs to be implemented as a separate process which takes input from certain other processes, performs the required processing and then returns the output to the next process:

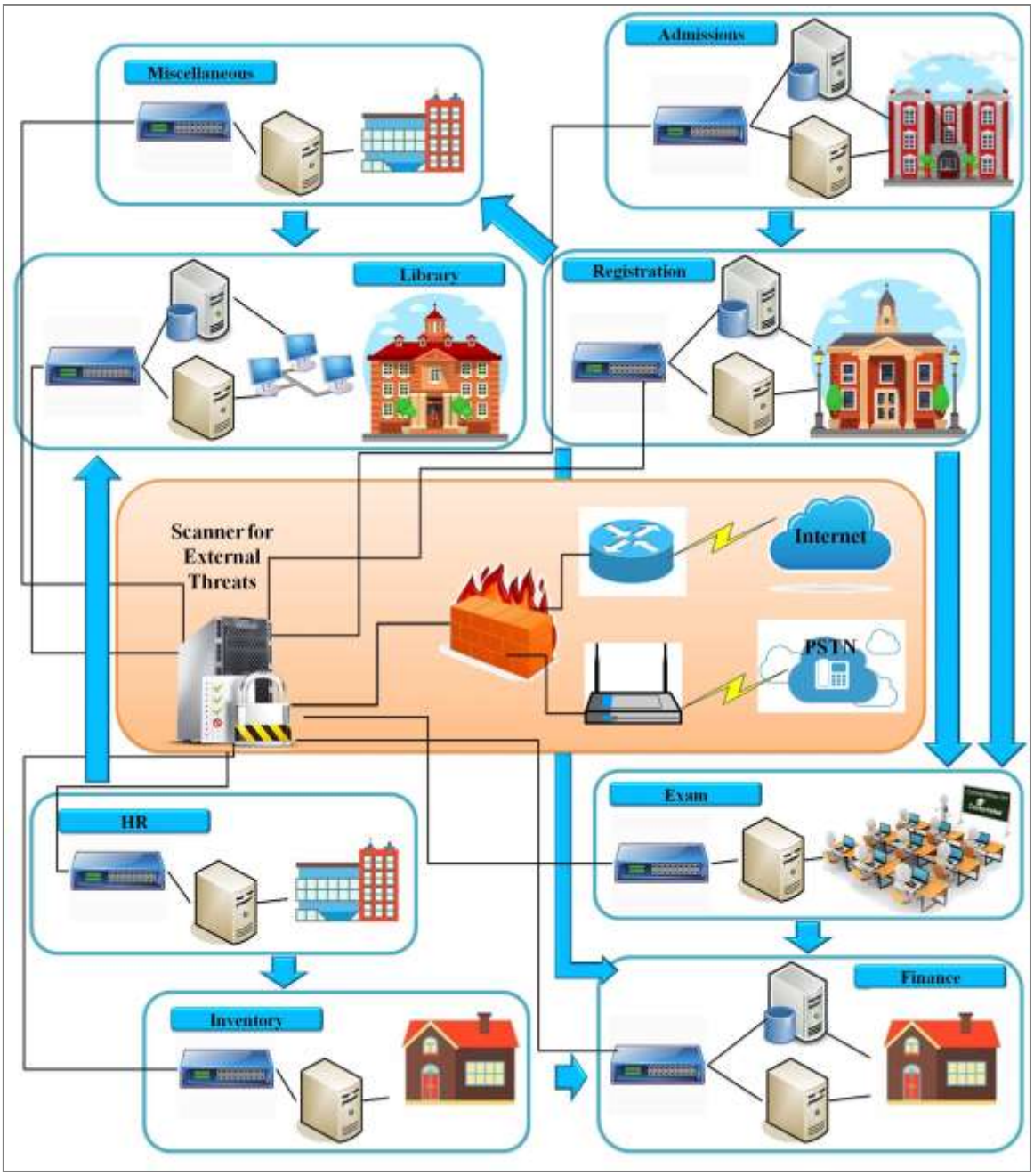

Figure 3.1: The Proposed Model for University

- According to our model, Admissions Module needs to be the very first module of the system which takes input of the applications of the candidates applying for the admissions. This module may take input either in the form of online admission process or from the admission office representative which has full rights to interpret the admissions data. Then this module can generate the admission test

slips for each student. Then this admissions information is passed to the Exam module which conducts the tests of these applying candidates, compiles the results and then sends back the results to the admissions module which publishes the results.

- After the selection of appropriate candidates, the result is forwarded to the registration module which is in the control of registration department of the university. The registration department is responsible for the verification of whole data provided by the admissions department in addition to the entry of all the possible academic, personal and demographic data about the students. Now once this data about the students is entered, it must be locked and made available to all the modules of the system with read only permissions. Users of those modules must be able to view this data without a permission to update this. The registration data update permissions must only be available to the registration department users with the appropriate log records of the updates and deletes.
- The exams module is for the purpose of students' assessment and evaluation. The rights of this module need to be scattered and distributed among different entities of the whole system. For example, preparation of the exam lists must be the responsibility of the respective faculty program coordinator. Teachers must be able to update the assessment records of the students including all their sessional marks and the end term marks. Sessional marks may include quizzes, assignments, class tests, lab tests and midterm etc. and final exam is the semester end term exam. After the entry of the assessment data, the information must be locked and must not even be possible for the teacher to update it. Assessment marks update permissions must be available for a specific user account, preferably exam department user account. At the end of the semester, whole assessment records must be available with the exam department to prepare the final results and declare it. The exam department must also be not allowed to make any assessment entry to the system. Rather they must only be capable of updating the records and this must be done based on an email generated by the respective teacher in consultation with the respective dean of the faculty. The record of this update request must be stored in the database.

- There needs to be an overall system auditor which checks all the updates made to the system daily with the help of an update report. This update report must be accompanied by the details of person who made the updates and the initiator of the update who made a request for the update.
- Similarly, finance module must be dealt with the assignment of appropriate roles and permissions to the finance department staff and for every student related transaction; an email must be sent automatically to the related students or in case of any other transactions, the appropriate email must be forwarded to the related persons with complete information. This will help quickly trace any malicious transactions made through the system and catch the culprit.
- Similar procedures must be applied for the other modules of the system and proper check and balance for each single activity of each module is quite important.
- Another important element of this model is the encryption of data during the communication process so that any network related intrusion during the data traffic may be avoided. Data must be transferred from one place to the other after performing the encryption and at the receiving end, this data must be decrypted.

The basic element of our proposed model is the development of an object-oriented approach which ensures the abstraction and data hiding of different objects/modules of this system. Each module is independent unit and the module specific data is only visible to the module members/users. No one else can have access to this data. There is no overlap of user permissions and usage rights are clearly assigned. Each module is treated as a separate process which takes input from certain other processes, performs the required processing and then forwards the output to another process. This ensures the smooth and reliable transmission of the data from one place to the other. Maintenance of the transactional logs is also highly recommended for each transaction along with the forwarding of email for the necessary transactions.

Figure 3.2 shows a diagram that presents a comprehensive picture of the proposed framework for security assessment. The *University IS Security* (UISS) framework is

adapted from that is composed of three major phases including (1) weak points identification, (2) matters prioritization, (3) security solutions. UISS aims to decrease risks of security breach. The first phase of the proposed model focuses on identifying weak points in university's environment while the second phase concentrates on the prioritizing the matters with higher risk and the last phase offers some security solutions for university's network.

The first step of the first phase is security requirement which provide information about the systems and the limitations and restrictions of IT systems. In the next step, threat scenarios are generated by listing the most common combinations of attack paths, attack goals and attack actor (attackers or hackers). In the final step of the first phase of UISS, the impact of exploit onto the system will be measured. In addition, authentication and authorization, intrusion detection, network filtering and routing, and encryption are considered in this step.

The second phase of UISS includes examination of frequency of exploit in which the probability that vulnerability can be exploited by the attacker is determined. In the examination of impact of exploit, the impact can be measured by using confidentiality impact, integrity impact, and availability impact metrics. In the final step of this phase, the level of security risk will be measured quantitatively. The risk level can be utilized into the creation of solutions.

The final phase of UISS is security solutions, which consists of a number of elements including data encapsulation, data encryption, inflow communication, user permissions, system auditor and email alerts. There are a number of modules within this information system which are the independent units and do not interfere in the functioning boundaries of each other. These modules or processes communicate with each other with the help of a solid communication system which also sets up the communication limitations.

In addition, some security solutions for cloud/network security, system security, and web security SQL injection are recommended to prevent university network from threats. Firewalls, regular network vulnerability scanning, Intrusion Detection Systems

(IDS) or Intrusion Prevention Systems (IPS), antivirus software for data processing servers, and workstations are recommended to improve cloud/network security. For system security, servers must backed up according to a regular schedule. In addition, servers must be configured in a way to capture who accessed a system and what changes were made. It is a good idea if the organization store backup offsite and the organization need to encrypt its backups. In order to enhance web security SQL injection, organization's website must have confidentiality and integrity. Organization's website must provide authentication to validate user names and passwords and also provide authorization to prevent attacker to change authorization information.

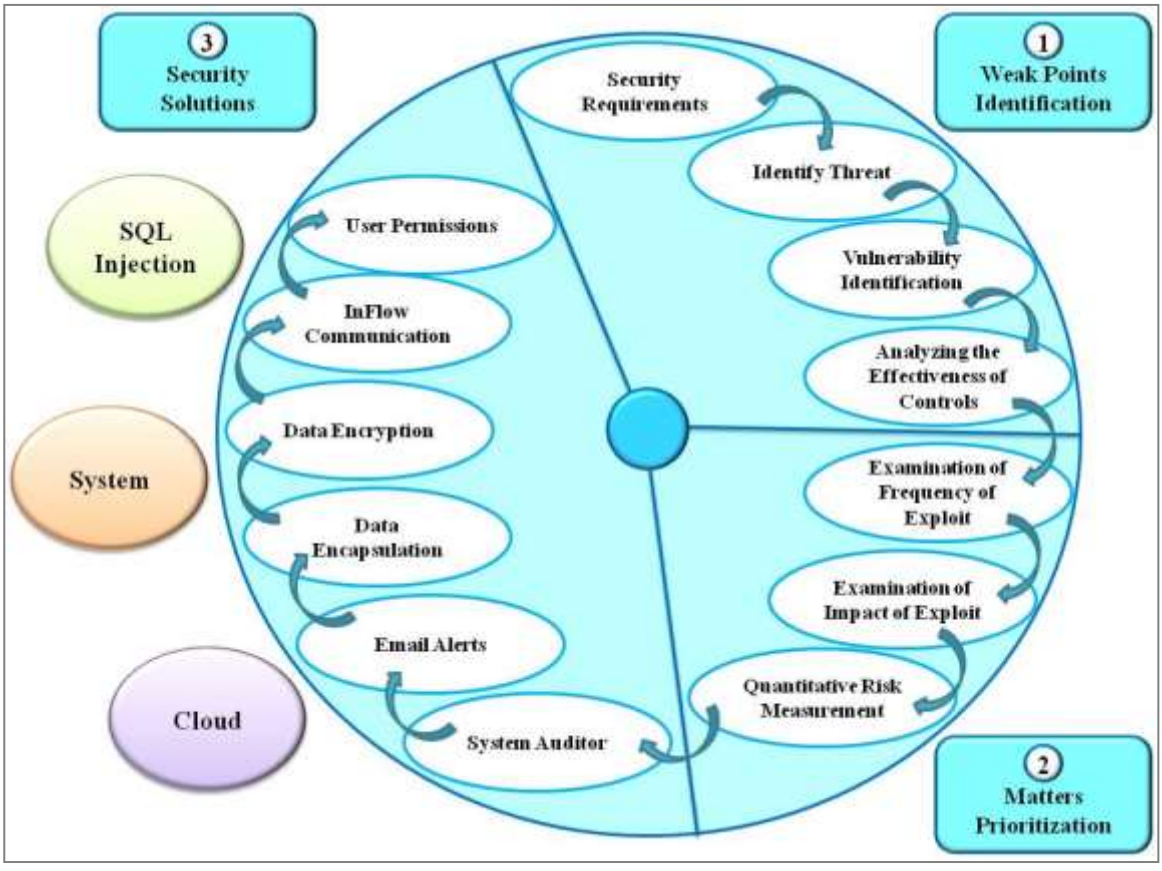

Figure 3.2: The Proposal model of University IS Security (UISS) Framework

Chapter 4 - DATA ANALYSIS & DISCUSSION

4.1. Introduction

This chapter reports the results of this study. Data was collected from five universities comprising Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University. The chapter is organized in four main sections. The next section introduces the main characteristics of the study sample. The subsequent three sections give, and elaborate on, results of this study. The results have been presented with reference to the three main research questions and, consequently, one section is devoted to each research question. Each of third and fourth sections has been divided into a number of sub-sections, corresponding to the number of secondary questions comprising each main research question. The fifth section discusses information security system of each university and the proposed model. The sixth section argues how to improve security in universities. Comparison between responses from each university is done in the next section followed by a summary of this chapter is given.

4.2. Main Characteristics of the Samples

The frequency distribution analysis (FDA) has been performed of the main characteristics of the study sample (age, gender and role). With reference to gender, the analysis outcomes (Table 4.1) reveal that 121 (76.6%) of the total 100 respondents were men while women were 37 participants only (23.4%) of the sample participants.

Table 4.1: Proportions of men and women in the study sample

Gender		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	121	76.6	76.6	76.6
	Female	37	23.4	23.4	100.0
	Total	158	100.0	100.0	

As regards age, outputs of FDA (Table 4.2) highlight that slightly less than half the respondents (75; 47.5%) belonged to the '17-25 Years' age group. Members of the '25-35 Years' age group rank second in number (37; 23.4% of all respondents). Sample members belonging to the '35-45 Years' age group were 31 persons (19.6%). Meantime, people who were older in age than 55 years were the lowest in number (2; 1.3%). People who were '45-55 Years' old counted 13 only, thus representing 8.2% of the study sample.

Table 4.2: Distribution of the sample respondents within the age groups

Age Group		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	17-25 Years	75	47.5	47.5	47.5
	25-35 Years	37	23.4	23.4	70.9
	35-45 Years	31	19.6	19.6	90.5
	45-55 Years	13	8.2	8.2	98.7
	> 55 Years	2	1.3	1.3	100.00
	Total	158	100.0	100	

As to the role (Table 4.3), it was found that the vast majority of the sample respondents were researcher (90; 57.0%) while only 25.3% and 7.6% of the participants were lecturer and team leader respectively. The least number of the sample participants were team member (11; 7.0%) and senior managers (5; 3.2%).

Table 4.3: Distribution of employees' role in AL Yamamah university

Role		Frequency	Percent
Valid	Team member	11	7.0
	Team leader	12	7.6
	Senior manager	5	3.2
	Lecturer	40	25.3
	Researcher	90	57.0
Total		158	100.0

4.3. Security and Responsibilities in All Five Universities

This section is intended to provide answers to the first research question: What are the genuine threats related to the security of universities' information systems data?

This section has been divided into two subsections talk about two secondary questions derived from the above question (first question), one on employees' awareness of information security and the second on who is the responsible of information security on the current system. Answers to both questions have been sought using FDA of the related data. The results are introduced next.

4.3.1. Information Security Awareness

This sub-section aims at introducing answer to the question: IS awareness among the universities personnel in different universities?

Answer to this question has been sought using FDA. The analysis results (Table 4.4) point out that level of awareness is not very common amongst Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University in Saudia Arabia who participated in this study. It was found that 87 participants (55.1%) strongly agreed that information security is an important part of their work, and 71 respondents (44.9%) agreed agreed on that. There is no respondent who does not consider the importance of information security in his/her work.

Table 4.4: Information security awareness

Information Security is an important part of my work.

Answer		Frequency	Percent	Valid Percent	Cumulative
Valid	Strongly Agree	87	55.1	55.1	100
	Agree	71	44.9	44.9	44.9
	Disagree	0	0	0	
	Strongly Disagree	0	0	0	
	Total	158	100.0	100.0	

4.3.2. The responsible of Information Security

This sub-section presents answer to the research question: who is the responsible party on the current system in all five universities?

The researcher was interested to identify the responsible party on the information security system in all five universities (Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University in Saudia Arabia). To this end, five options were listed in the survey (Appendix A) and responses of the sample members to these items were analyzed for frequency of distribution. The main findings were as follows (Table 4.5):

- All responsible parties were chosen by the respondent
- Each sample member used more than two major listed responsible parties.
- The responsible party which was chosen by the highest number of respondents (98; 62.0%) was the IT Services.
- The second most responsible party chosen was the departments that use data. This option was chosen by 37 individuals (23.4% of all respondents).
- Only 10 personnel (6.3%) choose deputy registrar's office, not to mention while only 8 respondents select managers and team leaders as responsible party of IS.
- Only 5 personnel (3.2%) think that the individual employee should be the responsible party.

Table 4.5: Distribution of the sample respondents according to responsible party of IS

Responsible party	Frequency	Percent
1. IT Services	98	62.0
2. Deputy Registrar's Office.	10	6.3
3. Departments that use data.	37	23.4
4. Managers and Team Leaders.	8	5.1
5. Individual Employees.	5	3.2

As shown in Table 4.6 majority of the respondents (124; 78.5%) did not receive any training on information security awareness. The foregoing findings illustrate that most of the sample members does not aware who should be responsible for the information security system.

Table 4.6: Received training on information security awareness

I have received Information Security awareness training at the University.

Receive Training		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	34	21.5	21.5	21.5
	No	124	78.5	78.5	100.0
Total		158	100.0	100.0	

Based on Table 4.7, all of the respondents (100.0%) from the sample members read and understood the policy and regulation governing use of computing facilities in their university.

Table 4.7: Understanding of policy and regulation of using the facilities

I have read and understood University Information Security Policy and Regulation Governing Use of Computing Facilities

Policy & Regulation		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	158	100	100	100
	No	0	0		
Total		158	100.0		

The researcher was interested in identifying the type of information that the sample members of study involved in their work. To this end, five options were listed in the survey (Appendix A) and responses of the sample members to these items were analyzed for frequency of distribution. The main findings were as follows (Table 4.8):

- All listed information types were involved by the respondents' work except none of the information types listed were involved in their work.
- The type of information which was involved by the highest number of respondents' works (121; 76.6%) was student IDs or personal details.
- The second most widely involved type of information was staff IDs or personal details. This type was involved by 36 individuals (22.8%)
- Financial information and research information were not involved in any respondents and only one respondent choose research information.

Table 4.8: Distribution of information type involved in the participants' work.

Information type	Frequency	Percent
1. Student IDs or Personal Details	121	76.6
2. Staff IDs or Personal Details.	36	22.8
3. Financial Information.	0	0
4. Research Information.	1	0.6
5. None of the above.	0	0

The foregoing findings illustrate that most of the sample participants of the study have critical information involved in their works, although, most of the sample participants lack the information security awareness and do not know much on the policy and regulation governing use of computing facilities in all universities as explain earlier under table 4.6 and 4.7 which led to the conclusion on the need of suitable information security model that overcome such challenges.

4.4. Security Threats in the Universities

This section sought answer to the question: What are the reasons of security threats?

This question has been fragmented by the researcher into two secondary questions and FDA was performed to provide answers to both. The main findings are presented in the sequent two sub-sections.

4.4.1. Handling the information

This sub-section tended to provide answer to the secondary question: What are security threats on handling the information among the personnel in all five universities?

Output of FDA (Table 4.9) uncover that the most of the sample respondents use their phone to send information which may contains names and other details. 81 respondents (51.3%) use E-mail message compared to lowest number of respondents (37; 23.4%), use Internet cloud service. The second highest method was the E-mail message with 68.0% of the participants. Internal cloud service was Hand deliver in hard copy or on USB (25.3%). No participant chooses phone and internal mail as appropriate method for sending information.

Table 4.9: You are asked to provide information containing names and contact details to another office. What is an appropriate method for sending this information?

Handling information options	Frequency	Percent
1. E-mail message	81	51.3
2. Internet cloud service	37	23.4
3. Phone	0	0
4. Hand deliver in hard copy or on USB	40	25.3
5. Internal mail	0	0

However, electronic and paper documents that may contain sensitive personal information such as names, pay grade, user codes or address did not handle by the participants' team in any special manner. Table 4.10 shows that all of the participants (158; 100.0%) says that documents handled by their teams are subjected to any internal procedures and policies to protect confidentiality while no participants says the opposite which, besides of the previous reason, answers a big part of the second research question as one of the reason of the security threats.

Table 4.10: Handling sensitive information

Electronic and paper documents may contain sensitive personal information e.g. names, pay grades, user codes, addresses etc. Which statement best describes how these documents are handled in your team?

Handling Manner	Frequency	Percent	Valid Percent	Cumulative Percent
Documents are subject to internal procedures and policies to protect confidentiality	158	100	100	100.0

Although, majority of the participants agreed (74.1% strongly agreed and 25.3% agreed) that they can play a significant role in protecting their work computers and information stored on it, they never remotely access the university's shared drive, files, application or emails (111; 70.3%) and almost every day for 46 of the participants (29.1%), see table 4.11 and 4.12.

Table 4.11: Individuals protecting their computers and data

I can play a significant role in protecting my computer and the information stored on it.

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	117	74.1	74.1	100.0
	Agree	40	25.3	25.3	25.9
	Disagree	1	0.6	0.6	0.6
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

Table 4.12: Remotely accessing the university shared drives, files, applications and emails

How often do you access University shared drives, files, applications or your emails remotely?

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Almost every day	46	29.1	29.1	29.1
	At least once a week	1	0.6	0.6	29.7
	At least once a month	0	0	0	0
	Never	111	70.3	70.3	100.0
	Total	100	100.0	100.0	

In the other hand, Table 4.13 illustrates that the majority of the sample participants of the study indicate that they have important information in their computers or immediate workspace that would be of any interest or values to others. 2.5% strongly agreed that they do not have information that would be of interest or values to others and almost the same (1.3%) for the sample participants who just agreed on that. However, 55.1% of the participants strongly disagree and indicates that they have information that would be of interest or values to others and almost the same (41.1%) goes for those who just disagree

Table 4.13: Important information that would be of interest or values to others

There is nothing on my work computer or in my immediate workspace that would be of any interest or value to others.

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	2.5	2.5	100.0
	Agree	2	1.3	1.3	97.5
	Disagree	65	41.1	41.1	96.2
	Strongly Disagree	87	55.1	55.1	55.1
	Total	100	100.0	100.0	

The foregoing findings illustrate that the above results gathered from the answers of all the questions in the questionnaire of this study are reasons that might make the handling

the information vulnerable to any security threats which might occur in the universities, which in turn will answer the second question of this research.

4.4.2. Computer Usage

This sub-section addresses the secondary question: What are the threats that lies on computers usage in five universities?

Outputs of FDA (Table 4.14) uncover that the overwhelming majority of the sample personnel (135; 85.4%) do not share the logins and passwords with their team members. This finding agrees with the findings presented in table 4.15 where the more than a half of the sample personnel (135; 85.4%) refused to provide their passwords when someone they know at work asked for it and stresses the fact about the security of information in terms of privacy and data safety which is considered one of the major obstacles that might lead to security threats. Although, 7 participants (4.4%) provided their passwords when they asked for it, 62 participants (39.2%) have never been asked for a password.

Table 4.14: Sharing login and passwords with the team

Does your team share logins and passwords?

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	23	14.6	14.6	14.6
	No	135	85.4	85.4	100
	Total	158	100.0	100.0	

Table 4.15: Providing password to a known collogue

Has anyone you know at work asked for your password?

Answers		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes and I provided it	7	4.4	4.4	4.4
	Yes and refused to provide it	89	56.3	56.3	60.8
	No	62	39.2	39.2	100.0
	Total	158	100.0	100.0	

The researcher was interested in identifying the action of the sample members when someone send an e-mail with attachment or link that is not work elated. To this end, four options were listed in the survey (Appendix A) and responses of the sample members to these options were analyzed for frequency of distribution. The main findings were as follows (Table 4.16):

- All listed responses were chosen by the respondents except always open the email if someone sends an attachment/link that is not work related.
- Only 6 sample members have chosen that they will always open emails with attachments or links that is not work related, 9.0% of the participants responds to open it very likely.
- The action which was chosen by the highest number of respondents' works (130; 82.3%) was not likely to open it. 17.1% of 27 participants chose possibly, depending on what is being sent.
- The above reflects that almost all sample personnel are aware of the spam and trap email that might lure someone to plant their malicious app or virus which may lead to a security threats. Though, this does not remove the fact that 17.1% of the sample participants might possibly fall in one of the email with fraud attachment or links.

Table 4.16: If someone e-mails you an attachment/link that is not work related, how likely are you to open it?

Participants responds	Frequency	Percent
1. Not likely	130	82.3
2. Possibly, depending on what is being sent.	27	17.1
3. Very likely.	1	0.6
4. Always.	0	0

4.5. Improving Security

In order to improve security in the university network, cloud security, system security and Web security SQL injection are considered in this study.

4.5.1. Cloud/Network Security

Firewall and VPN are two important options to improve cloud/network security. Based on the survey results from five universities (Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University in Saudia Arabia), all of the respondents ensure that network boundaries protected by firewalls in their university. On the other hand, most of the respondents (111; 70.3%) believed that employees do not required to use a VPN when accessing the organization's systems from all remote locations whereas 47 of the respondents (29.7%) believed vise versa (Table 4.17).

Table 4.17: Cloud/Network Security 1

Are network boundaries protected by firewalls in your university?

Answers		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	158	100	4.4	100.0
	No	0	0	0	0
	Total	158	100.0	100.0	

Are employees required to use a VPN when accessing the organization's systems from all remote locations?

Answers		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	47	29.7	29.7	29.7
	No	111	70.3	70.3	100.0
	Total	158	100.0	100.0	

Intrusion Detection Systems (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations while Intrusion Prevention Systems (IPS) is a preemptive approach to network security used to identify potential threats and respond to them swiftly. As illustrated in Table 4.18, regular network vulnerability scanning, IDS or IPS are required for cloud/network security and most of the respondents are either agree or strongly agree in this regards. In addition, antivirus software must be installed on data processing servers and workstations.

Table 4.18: Cloud/Network Security 2

Regular network vulnerability scanning is required.

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	71	44.9	44.9	100.0
	Agree	87	55.1	55.1	55.1
	Disagree	0	0	0	0
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are required for my organization.

Answer		Frequency	Percent	Valid Percent	Cumulative
Valid	Strongly Agree	120	75.9	75.9	100.0
	Agree	38	24.1	24.1	24.1
	Disagree	0	0	0	0
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

Antivirus software must be installed on data processing servers.

Answer	Frequency	Percent	Valid Percent	Cumulative	Answer
Valid	Strongly Agree	81	51.3	51.3	100.0
	Agree	77	48.7	48.7	48.7
	Disagree	0	0	0	0
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

Antivirus software must be installed on workstations.

Answer	Frequency	Percent	Valid Percent	Cumulative	Answer
Valid	Strongly Agree	113	71.5	71.5	100.0
	Agree	45	28.5	28.5	28.5
	Disagree	0	0	0	0
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

4.5.2. System Security

Server backup is needed according to a regular schedule to improve system security. As shown in Table 4.19, 50% of the respondents are strongly agree and 48.7% are agree to have server backup according to a regular schedule. Only two respondents disagree to have regular server backup. In addition, most of the respondents are either agree (114; 72.2%) or strongly agree (44; 27.8%) that servers must be configured in a way to capture who accessed a system and what changes were made. The respondents believe that it is a good idea if the organization store backup offsite and the organization need to encrypt its backups.

Table 4.19: System Security

Computer systems (servers) must backed up according to a regular schedule.

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	79	50.0	50.0	100.0
	Agree	77	48.7	48.7	50.0
	Disagree	2	1.3	1.3	1.3
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

Servers must be configured in a way to capture who accessed a system and what changes were made.

Answer		Frequency	Percent	Valid Percent	Cumulative
Valid	Strongly Agree	44	27.8	27.8	27.8
	Agree	114	72.2	72.2	100
	Disagree	0	0	0	0
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

It is a good idea if the organization store backup offsite.

Answer	Frequency	Percent	Valid Percent	Cumulative	Answer
Valid	Strongly Agree	81	51.3	51.3	100.0
	Agree	77	48.7	48.7	48.7
	Disagree	0	0	0	0
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

The organization need to encrypt its backups.

Answer	Frequency	Percent	Valid Percent	Cumulative	Answer
Valid	Strongly Agree	82	51.9	51.9	100.0
	Agree	75	47.5	47.5	48.1
	Disagree	0	0	0	0
	Strongly Disagree	1	0.6	0.6	0.6
	Total	158	100.0	100.0	

4.5.3. Web Security SQL Injection

SQL Injection is a type of injection or attack in a Web application, in which the attacker provides Structured Query Language (SQL) code to a user input box of a Web form to gain unauthorized and unlimited access. Table 4.20 shows respondents' opinions about confidentiality of organizations' website, authentication to validate user names and passwords, and authorization to prevent attacker to change authorization information. Majority of the respondents are strongly disagree (97;61.4%) and disagree (44; 27.8) respectively about organization's website to have confidentiality which could be viewed by unauthorized users. All respondents believe that organization's website must have integrity to prevent external source to make unauthorized modifications such as altering or even deleting information from target databases except 19 of them (12%). Furthermore, respondents prefer organization website to provide authentication (73.4% strongly agree, 25.9% agree, and 0.6% disagree) to validate user names and passwords and authorization (51.9% strongly agree and 48.1 agree) to prevent attacker to change authorization information.

Table 4.20: Web Security SQL Injection

Organization's website must have confidentiality which could be viewed by unauthorized users.

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	13	8.2	8.2	100.0
	Agree	4	2.5	2.5	91.8
	Disagree	44	27.8	27.8	89.2
	Strongly Disagree	97	61.4	61.4	61.4
	Total	158	100.0	100.0	

Organization's website must have integrity to prevent external source to make unauthorized modifications such as altering or even deleting information from target databases.

Answer		Frequency	Percent	Valid Percent	Cumulative
Valid	Strongly Agree	55	34.8	34.8	100.0
	Agree	84	53.2	53.2	65.2
	Disagree	0	0	0	0
	Strongly Disagree	19	12	12	12
	Total	158	100.0	100.0	

Organization's website provides authentication to validate user names and passwords.

Answer	Frequency	Percent	Valid Percent	Cumulative	Answer
Valid	Strongly Agree	116	73.4	73.4	100.0
	Agree	41	25.9	25.9	26.6
	Disagree	0	0	0	0
	Strongly Disagree	1	0.6	0.6	0.6
	Total	158	100.0	100.0	

Organization's website provides authorization to prevent attacker to change authorization information.

Answer	Frequency	Percent	Valid Percent	Cumulative	Answer
Valid	Strongly Agree	82	51.9	51.9	100.0
	Agree	76	48.1	48.1	48.1
	Disagree	0	0	0	0
	Strongly Disagree	0	0	0	0
	Total	158	100.0	100.0	

The results of security improvement section indicate the need of cloud/network security, system security and web security SQL injection in universities' network. Based on the results firewall and VPN are two important options to improve cloud/network security. Additionally, regular network vulnerability scanning, IDS or IPS are required to improve cloud/network security. Antivirus software must be installed on data processing servers and workstations. For enhancing system security in universities, server backup is needed according to a regular schedule. Servers must be configured in a way to capture who accessed a system and what changes were made. Furthermore, the organizations must store backup offsite and the organizations need to encrypt its backups. Finally, in order to improve web security SQL injection, confidentiality of organizations' website, authentication to validate user names and passwords, and authorization to prevent attacker to change authorization information are needed.

4.6. Comparison between Five Universities

The frequency distribution analysis (FDA) has been performed of the main characteristics of the study sample for each university (age, gender and role). With reference to gender, the analysis outcomes (Table 4.21) reveal that majority of the respondents from five universities (Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University) were male as female respondents are only from Princess Noura University (33.3%) and Al-Madinah International University (18.9%). Generally, 76.6% are male while 23.4% are female.

Table 4.21: Gender Comparison Among Five Universities

Gender		Frequency	Percent	Valid Percent	Cumulative Percent
Princess Noura University	Male	20	66.7	100.0	100.0
	Female	10	33.3		
	Total	30	100.0		
King Saud University	Male	32	100.0	100.0	100.0
	Female	0			
	Total	32			
Imam Muhammad bin Saud University	Male	30	100.0	100.0	100.0
	Female	0			
	Total	30			
Arab Open University	Male	29	100.0	100.0	100.0
	Female	0			
	Total	29			
Al-Madinah International University	Male	30	81.1	81.1	81.1
	Female	7	18.9	18.9	100.0
	Total	37	100.0	100.0	
Total	**Male**	**121**	**76.6**	**76.6**	**76.6**
	Female	**37**	**23.4**	**23.4**	**100.0**
	Total	**158**	**100.0**	**100.0**	

Summarizing quantitative information in order to understand characteristics of entire population or a sample of it in a given situation is called descriptive analysis. It can provide valuable information about the study variables to show their truth (Kohler & Kreuter, 2005). Minimum, maximum, mean, and standard deviation can be used to report the results of descriptive analysis. Mean is used to evaluate central tendency while standard deviation depicts dispersion of distribution and assesses the variance from the mean. The results of security and responsibilities in five universities are compared in Table 4.22. The outcomes reveal that information security is more important for Arab Open University (mean: 4.62) and less important for Al-Madinah International University (mean: 4.48); however, the difference is not significant.

Table 4.22: Security and Responsibilities in Five Universities

Information Security is an important part of my work.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.50	0.50	4	5
King Saud	4.59	0.49	4	5
Imam Muhammad	4.56	0.50	4	5
Arab Open	4.62	0.49	4	5
Al-Madinah	4.48	0.50	4	5

As shown in Table 4.23, the most participants, who are agree on their significant role in protecting their computer and the information stored on it, are from King Saud University (mean: 4.87) followed by Imam Muhammad University (mean: 4.83) and Princess Noura (mean: 4.76) respectively. In addition, most of the participants from Princess Noura University (2.03) disagree that there is nothing on their work computer or in their immediate workspace that would be of any interest or value to others.

Table 4.23: Individuals protecting their computers and data

I can play a significant role in protecting my computer and the information stored on it.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.76	0.43	4	5
King Saud	4.87	0.33	4	5
Imam Muhammad	4.83	0.59	2	5
Arab Open	4.56	0.50	4	5
Al-Madinah	4.48	0.50	4	5

There is nothing on my work computer or in my immediate workspace that would be of any interest or value to others.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	2.03	1.42	1	5
King Saud	1.40	0.49	1	2
Imam Muhammad	1.43	0.50	1	2
Arab Open	1.37	0.49	1	2
Al-Madinah	1.5	0.50	1	2

One of the main important parts of security is related to cloud/network security especially for university network. For this reason, it is included in the survey to find respondents opinion about cloud/network security. Regular network vulnerability scanning is one of the important factors of cloud/network security. The results of this research indicate that almost all of the participants from five universities agree that regular network vulnerability scanning is required for their university network as shown in Table 4.24; however, the respondents in Arab Open University (mean:4.65) and Al-Madinah International University (mean:4.44) are more agree on vulnerability of network. Other parameters of cloud/network security are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) which have more agree on among the respondents in Imam Muhammad University and King Saud University respectively. In addition, the respondents especially from Arab Open University (mean: 4.65) and Imam Muhammad University (mean: 4.90) believe that antivirus software must be installed on data processing servers and workstations to improve cloud/network security.

Table 4.24: Cloud/Network Security

Regular network vulnerability scanning is required.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.43	0.50	4	5
King Saud	4.31	0.47	4	5
Imam Muhammad	4.36	0.49	4	5
Arab Open	4.65	0.48	4	5
Al-Madinah	4.44	0.49	4	5

Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are required for my organization.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.66	0.47	4	5
King Saud	4.87	0.33	4	5
Imam Muhammad	4.96	0.18	4	5
Arab Open	4.72	0.45	4	5
Al-Madinah	4.76	0.42	4	5

Antivirus software must be installed on data processing servers.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.50	0.50	4	5
King Saud	4.43	0.50	4	5
Imam Muhammad	4.40	0.49	4	5
Arab Open	4.65	0.48	4	5
Al-Madinah	4.57	0.50	4	5

Antivirus software must be installed on workstations.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.56	0.50	4	5
King Saud	4.84	0.36	4	5
Imam Muhammad	4.90	0.30	4	5
Arab Open	4.72	0.45	4	5
Al-Madinah	4.57	0.50	4	5

System security is considered as another part of improving security in university network. System security comprises servers backed up according to a regular schedule, correct server configuration, storing backup offsite, and backup's encryption. Among all respondents, those from Imam Muhammad University are more agree on server backup

according to a regular schedule (mean: 4.83), server configuration (mean: 4.93) and backup's encryption (mean: 4.86). The results of system security questions among all five universities are indicated in Table 4.25.

Table 4.25: System Security

Computer systems (servers) must backed up according to a regular schedule.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.33	0.80	2	5
King Saud	4.40	0.49	4	5
Imam Muhammad	4.83	0.59	2	5
Arab Open	4.65	0.48	4	5
Al-Madinah	4.56	0.50	4	5

Servers must be configured in a way to capture who accessed a system and what changes were made.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.63	0.49	4	5
King Saud	4.87	0.33	4	5
Imam Muhammad	4.93	0.25	4	5
Arab Open	4.72	0.45	4	5
Al-Madinah	4.48	0.50	4	5

It is a good idea if the organization store backup offsite.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.50	0.50	4	5
King Saud	4.37	0.49	4	5
Imam Muhammad	4.50	0.50	4	5
Arab Open	4.65	0.48	4	5
Al-Madinah	4.43	0.50	4	5

The organization need to encrypt its backups.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.46	0.81	1	5
King Saud	4.84	0.36	4	5
Imam Muhammad	4.86	0.34	4	5
Arab Open	4.72	0.45	4	5
Al-Madinah	4.48	0.50	4	5

Web Security SQL Injection is another important part of security in university network. Most of the respondents from five universities believed that organization's website must have confidentiality which could not be viewed by unauthorized users. Among all of the participants, those who are from Imam Muhammad University (mean: 1.46) strongly disagree with viewing website confidentiality by unauthorized users. After Imam Muhammad University, the participants from Arab Open University (mean: 1.62) and Al-Madinah International University (mean: 1.64) are stricter in this regards. In addition, only participants from Arab Open University and Al-Madinah International University agree on integrity of organization's website. The rest of participants from other universities do not agree with integrity option. Majority of the participants from all five universities agree that organization's website provides authentication to validate user names and passwords and organization's website must provides authorization to prevent attacker to change authorization information.

Table 4.26: Web Security SQL Injection

Organization's website must have confidentiality which could be viewed by unauthorized users.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	2.00	1.57	1	5
King Saud	1.68	1.25	1	5
Imam Muhammad	1.46	1.04	1	5
Arab Open	1.62	0.94	1	5
Al-Madinah	1.64	0.95	1	5

Organization's website must have integrity to prevent external source to make unauthorized modifications such as altering or even deleting information from target databases.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	3.66	1.42	1	5
King Saud	3.87	1.18	1	5
Imam Muhammad	1.43	0.50	1	5
Arab Open	4.10	1.34	1	5
Al-Madinah	4.21	0.91	1	5

Organization's website provides authentication to validate user names and passwords.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.60	0.81	1	5
King Saud	4.78	0.42	4	5
Imam Muhammad	4.90	0.30	4	5
Arab Open	4.72	0.45	4	5
Al-Madinah	4.59	0.49	4	5

Organization's website provides authorization to prevent attacker to change authorization information.

University	Mean	Std. Deviation	Minimum	Maximum
Princess Noura	4.46	0.50	4	5
King Saud	4.50	0.50	4	5
Imam Muhammad	4.46	0.50	4	5
Arab Open	4.65	0.48	4	5
Al-Madinah	4.51	0.50	4	5

4.7. Discussion

The subject University of this Study, offers its own significant environments and culture. However, during our research it was found that there is no particular breach of information system security in university. During our survey, it was identified that there have been few events where employees were found to be responsible any malicious information security and strict action was taken against them. One expert in his interview told the researcher that the employees associated with the information system can affect the information system security either intentionally or unintentionally. The expert further added that the breach of information security affects the credibility of the universities, emotions and knowledge of the users. The lack of trust in any information system restricts the operational scope of the system. The universities have a great dependence on their information system.

The main duty of the IT department in the university is the data base management. Information security is the primary concern in the university and a major part of the day is spent in dealing with the management of security related issues. The information security risk management measures are applied in the entire main and support process without any exception. This is because the information security is essential for safety, revenue, loss prevention, inefficiency and negative publicity, etc. the interviews with the experts and staff responsible provided us with the following insight to the mandatory requirements for the information security system within the universities.

- In the university, the employees are required to sign a confidentiality agreement. With this agreement, they become accountable for any breach of information system security.

- The end user is aware of the security related regulations. They are expected to follow this regulation without any exception. A special emphasis is made on the employee to read each line before signing the confidentiality agreement. This makes the things more clear and transparent about the university expectation regarding the information security system.

- Proper training is provided to the employee for the data base managements and surveillance. The university wants to secure the information available. This is not only necessary for the smooth operation, but also for trust and good will.

- The employees of the IT department are provided with satisfying pay and rewards to motivate them to work with devotion. This not only motivates the employees, but also makes sure that they are not tempted with money to breach the information security system.

- It was noticed that in the university, there exist a culture of internal security. The employees understand and respect the security protocol of the university. The management also considers it to be responsibility.

- The access rights to the information system are customized. There are different provisions available in different logins. The administration rights are only limited to selected user can access and change the information in the data basis.

- The information surveillance is monitored with the help of check and balance. A proper record is maintained of the entire login with exact time and activities. Not only that the surveillance cameras are also installed in the IT department and are monitored around the clock.

- The students were confident about the information system and its security.

- The information system plays an important role in the efficiency of the university performance. It provides the detailed information about the students and also help the teacher in providing detailed and prompt feedback to the student on his/ her performance. It bridges all the communication gaps and the students and teacher can keep in touch very easily. It security can be one concern, but the students and the teachers consider it essential for university's operations and processes.

- According to the users the rules and regulation of the information system security was exclusive to the IT staff and they don't have sufficient knowledge about it. Universities are the building pillars of any nation. They have the responsibilities for the present and the future of the nation.

- It has been observed that the development tasks of the information systems are in the hands of selected individuals and they can control everything. If they leave the work pool, the whole system suffers and a lot of time is required for the proper replacement. This mean time results in lots of security threats and can be exploited by the ones intending to target the system

- When development process or any user transactional process is stuck at any stage because of any permissions, then rather than devising a permanent solution, the IS administration temporarily disable the security restrictions and allow the users to carry on with their required tasks and then reassign the restrictions. This results in great inconsistency of data as well as threats to the data.

- Although usage log is maintained by the systems but system administrations have the facility to get into the database directly and they can easily make any types of changes which are not traceable. Thus, any data administrator with bad intentions can easily victimize the authenticity of the data.

- Security measures at times also become a hurdle in the smooth functioning of the tasks and users become dependent on the IS staff to resolve their issues. This wastes a lot of their time. For example, if the system bars the user to perform a specific task, they must also be allowed to handle exceptional cases when required and the records of all the exceptional transactions must be maintained with the user logs.

- There is not much clarity about the usage rights of the system. For example, course registration and student registration are allowed to both the registration department and the program coordinator in the respective faculties, in some cases. This can result in data inconsistency and also untraceable data mistakes.

- If any error is found in the data, it is quite tedious and time consuming task to identify the correct place and responsibility of the error because of absence of any proper mechanism.

- There are a lot of additions and modifications required to let these systems work appropriately as these are in the initial stages relatively. But available staff is insufficient to incorporate these changes. As a result, most of the tasks are being performed on ad hoc basis rather than finding a permanent solution of the problems. For example, if some teacher requires a specific report and that is not available, the IS staff develops a temporary report for that time and an effort is not made to make this report a permanent part of the whole system which may be utilized by other teachers at any other time. This result in the wastage of resources and the staff is left with the less time to focus on security issues. Rather they are more occupied with such repetitive tasks.

As mentioned above, in order to improve security in any university network, there are important parameters related to cloud/network security, system security and web security SQL injection. The results of the survey are compared among all five universities and the main important parameters are mentioned based on the results. Therefore, based on the need and preference of the participants from each university, the main security parameters can be revealed and therefore enhanced in each university.

4.8. Summary

The information system plays an important role in performance and efficient working of the universities. This study has identified the security measures applied by the

IS departments of some selected universities and has also highlighted some of the potential threats to their data and data processing activities. These findings will be interpreted and analyzed in the next chapter which will conclude the findings of this research.

Chapter 5 - FINDINGS AND CONCLUSIONS

5.1. Introduction

Information System security plays a very important role in the smooth functioning of all the activities of a university as whole infrastructure is dependent on this system. Now information systems are utilized by virtually all the employees of the universities and their performance is dependent on the correct functioning of these systems. If systems work fine and according to the requirements, then overall output of the organization is increased otherwise it results in the degradation of the overall organizational output.

This study has intended to highlight the IS security concerns in the universities keeping in view the great importance of university data which may result in quite bad consequences if not utilized properly. The study has selected one university of Saudi Arabia and then selected some respondents from this university to respond to the questionnaires and the interviews. An observation of the existing systems was also made and some major leakages in the systems were highlighted. It was found that normal users were satisfied on average with the security measures but in fact this was because of lack of awareness with the appropriate IS practices. These systems have some potential threats which get out of the sight of the normal users but these are actually harming the systems. These issues include the temporary solutions from the IS staff to support the users, hacker's intrusion into the systems, lack of appropriate user permissions, unawareness among the staff, temporarily lifting of security measures etc.

The information systems of the universities need to be quite safe and secure before carrying on the transactions over it. The following section will describe strengths and weaknesses of our proposed model of information systems application in the university.

5.2. Strengths and Weaknesses of the Model

5.2.1. Strengths

We can highlight the strengths of our proposed model as follows:

- It is easy to be developed within a distributed environment where work can be distributed among different development units such that development of every unit leads to the attainment of the overall objectives
- The module specific information is encapsulated within that specific module and cannot be directly accessed by any other module. All the exchange of information is performed with the help of a secure communication channel and all the transactions of this communication channel are recorded.
- The communication channel is established in a flow which restricts the access to data from the unauthorized sources. For example, the data prepared by the admissions department is only accessible to two departments i.e. exam department and the registration department. The exam department will use this data for the conduct of admission tests and registration will be able to register the successful candidates as the students of the university. Other departments like finance department will not be able to have access to this data. They will be able to use only students' data provided by the registration department.
- All the transactions will be performed by the module specific users and these will be recorded, it will be quite easy to trace any changes made to the data at any time. This will ensure that any unauthorized changes cannot be made to the data.
- There is no overlap of user permissions. Permissions are assigned to the users exclusively. Therefore, no change in the system is untraceable. Certain users will be able to view data, others will be able to add the data and some other users will have additional rights to even update the data.
- The model also proposes the need of an overall system auditor which checks all the updates made to the system daily with the help of an update report. This update report must be accompanied by the details of the person who made the updates and the initiator of the update who made a request for the update.
- The model also proposes the issuance of an email alert to the stakeholders in case of important updates to the system. On the receiving of email, the users will be able to confirm that whether this update has been made by them or someone else.

This is also an additional function which secures from the happening of any unauthorized update.

5.2.2. Weaknesses

We can list down the weaknesses of the system as follows:

- Although application of data encapsulation is ideal but on the practical grounds it is not easy to implement it and there may arise the situations where one process may need to have direct access to the data of another process
- There are always exceptional cases during any process which make it difficult to set up some fixed permissions and not to allow their violation.
- Involvement of System Auditor cannot be considered as a very healthy practice as it may lead to the manual processing of information which may result in delays.
- Arrival of too many email alerts can cause the frustration of the users and they may underestimate its importance.

5.3. Contribution of this study

This study has provided an in-depth insight of the required security measures necessary for the implementation of Information Systems security in the universities. The model proposed by this study is an object based model which emphasizes the isolation of each module from the other modules and to reflect it as an entity. Application of the recommendations of this study can greatly enhance the reliability and authenticity of the information systems of the universities and will enable these systems to be the safe places of data storage, retrieval and processing.

The *University IS Security* (UISS) was proposed to prevent security threats in universities network. The framework includes three major phases including (1) weak points identification, (2) matters prioritization, (3) security solutions. In addition, some security recommendations for cloud/network security, system security and web security SQL injection are added into the framework based on the survey results. The framework can be used in universities to enhance their security against internal and external threats.

Implementation of proposed model will ensure that there will be no existence of loopholes like data transportation stealing, unauthorized data access, data inconsistency and overlapping of usage rights. These loopholes are common in the existing systems, raising questions on the integrity of these systems.

5.4. Future Work

This study has highlighted the issues and concerns related to the university information systems and provided a security roadmap for the successful implementation of the whole system. Following are some of the likely future works which we can carry on later.

- A quantitative research may be performed in order to get a broader level of understanding of the issues and concerns of the IS users and university executives. This will ensure the much more reliable and authentic solutions for the security threats because the concerns identified will be much more quantifiable.
- A separate study may be conducted on the issue of intrusions into five universities information systems in order to perform malicious activities and compare the results from each university.
- Any good study exploring the general information system security threats may be extended further to the educational systems security threats. This will provide a broader spectrum of the whole problem.

5.5. Conclusion

This study has analyzed the security situation of the information systems of the universities in order to come up with the identification of any known and unknown threats to the university data and then to propose some solutions to meet this critical problem.

The study performed the data collection with the help of surveys and interviews. These helped understand the genuine issues and concerns faced by the users of the system and the likely damages that this data insecurity was supposed to create. Then the study explored the reasons of these threats which were the lack of information security awareness, handling the information using phones, the shared credential for computer access, not mention, the lack of system modules that makes every department independent in terms of access right and permission. At the end, the study came up with a security model which can address the issues of the data security. The security model proposed by this study is an object-oriented model in which different modules of the system act as objects in the form of independent processes, having input from different sources, processing the input and outputting the results to another process. This ensures the isolation of the modules and their data abstraction. The study also emphasized on the enforcement of the proper check and balance over each transaction being performed on the system and logging each single activity and generating appropriate activity alerts.

Even the survey was conducted in five universities (Princess Noura University, King Saud University, Imam Muhammad bin Saud University, Arab Open University, and Al-Madinah International University in Saudi Arabia), the results was almost the same from each university. Most of the respondents agree to have cloud/network security, system security and web security SQL injection. They believe that firewalls, regular network vulnerability scanning, Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), antivirus software for data processing servers, and workstations are required to improve cloud/network security. In addition, for system security, servers must backed up according to a regular schedule and configured in a way to capture who accessed a system and what changes were made. It is a good idea if the organization store backup offsite and the organization need to encrypt its backups. In order to enhance web security SQL injection, organization's website must have confidentiality and integrity. Organization's website must provide authentication to validate user names and passwords and also provide authorization to prevent attacker to change authorization information.

Overall findings of this study can hold a great value for not only the universities but for any form of educational institutions which implement the information systems and this can be a source of great satisfaction for the educational executives who seek to deploy reliable communication infrastructure within their organization.

REFERENCES

Alfawaz, S., May, L. J., & Mohannak, K. (2008). E-government security in developing countries: A managerial conceptual framework.

Aljohani, A. M., Peng, A., & Nunes, M. (2015). Critical factors leading to ERP replacement in Higher Education Institutions in Saudi Arabia: preliminary results. *iConference 2015 Proceedings*.

Alsultanny, Y. A. (2014). Assessment of E-Government Weak Points to Enhance Computer Network Security. *International Journal of Information Science, 4*(1), 13-20.

Altamimi, A., & Eavis, T. (2012). Securing Access to Data in Business Intelligence Domains.

Alwi, N. H. M., & Fan, I.-S. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS), 1*(2), 148-156.

Amoako-Gyampah, K., & Salam, A. F. (2004). An extension of the technology acceptance model in an ERP implementation environment. *Information & Management, 41*(6), 731-745.

Avgerou, C., & Cornford, T. (1998). *Developing information systems: concepts, issues and practice*: Palgrave Macmillan.

Bernroider, E. W. (2008). IT governance for enterprise resource planning supported by the DeLone–McLean model of information systems success. *Information & Management, 45*(5), 257-269.

Bhilare, D. (2013). Information Security Preparedness of Indian Academic Campuses with respect to Global Standards: a Gap Analysis. *International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2*(11).

Bologa, A., Muntean, M., Sabau, G., & Scorta, I. (2009). Critical implementation factors in higher education ERPs. Paper presented at the *Proceedings of the 8th WSEAS international conference on Artificial intelligence, knowledge engineering and data bases*, (pp. 441-446). World Scientific and Engineering Academy and Society (WSEAS).

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. *The International Review of Research in Open and Distributed Learning, 14*(5).

Dia, O. A., & Farkas, C. (2015). Risk Aware Query Replacement Approach for Secure Databases Performance Management. *IEEE Transactions on Dependable and Secure Computing, 12*(2), 217-229.

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security, 11*(3), 106-114.

Furnell, S., & Karweni, T. (2001). Security issues in online distance learning. *Vine, 31*(2), 28-35.

Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics, 2*(5), 544-554.

Jahid, S., Gunter, C. A., Hoque, I., & Okhravi, H. (2011). MyABDAC: compiling XACML policies for attribute-based database access control. Paper presented at

the *Proceedings of the first ACM conference on Data and application security and privacy*, (pp. 97-108). ACM.
Jones, D. S. (1979). *Elementary information theory*: Clarendon Press.
Kabra, G., Ramamurthy, R., & Sudarshan, S. (2006). Redundancy and information leakage in fine-grained access control. Paper presented at the *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, (pp. 133-144). ACM.
Kambourakis, G. (2013). Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art. *International Journal of u-and e-Service, Science and Technology, 6*(3), 67-84.
Khajaria, K., & Kumar, M. (2011). Modeling of security requirements for decision information systems. *ACM SIGSOFT Software Engineering Notes, 36*(5), 1-4.
Kim, H.-W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS quarterly*, 567-582.
Kindy, D. A., & Pathan, A.-S. K. (2011). A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques. Paper presented at the *Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on*, (pp. 468-471). IEEE.
Kohler, U., & Kreuter, F. (2005). *Data analysis using Stata*: Stata press.
Krishnan, K. (2013). Chapter 6 - Data Warehousing Revisited *Data Warehousing in the Age of Big Data* (pp. 127-145). Boston: Morgan Kaufmann.
Kumar, M., Gosain, A., & Singh, Y. (2010). Stakeholders driven requirements engineering approach for data warehouse development. *Journal of Information Processing Systems, 6*(3), 385-402.
Kumar, M., Gosain, A., & Singh, Y. (2014). Empirical validation of structural metrics for predicting understandability of conceptual schemas for data warehouse. *International Journal of System Assurance Engineering and Management, 5*(3), 291-306.
Kvavik, R. B., & Voloudakis, J. (2003). *Information technology security: Governance, strategy, and practice in higher education*: Educause.
Kwahk, K.-Y., & Lee, J.-N. (2008). The role of readiness for change in ERP implementation: Theoretical bases and empirical validation. *Information & Management, 45*(7), 474-481.
Liu, Q., Zhang, X., Chen, X., & Wang, L. (2014). The resource access authorization route problem in a collaborative manufacturing system. *Journal of Intelligent Manufacturing, 25*(3), 413-425.
Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications, 36*(1), 42-57.
Nanda, A. (2005). Encrypt Your Data Assets. *Oracle Magazine, 19*(1), 61-64.
Oblinger, D. (2003). Computer and network security and higher education's core values. *Research Bulletin*(6).
Olugbara, O. O., Kalema, B. M., & Kekwaletswe, R. M. (2014). Identifying critical success factors: The case of ERP systems in higher education.
Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. *European journal of information systems, 17*(3), 236-263.

Schniederjans, D., & Yadav, S. (2013). Successful ERP implementation: an integrative model. *Business Process Management Journal, 19*(2), 364-398.
an analysis and synthesis of the literature. *Journal of Information Technology, 32*(2), 147-162.
Yang, C., Lin, F. O., & Lin, H. (2002). Policy-based privacy and security management for collaborative E-education systems. Paper presented at the *Proceedings of the 5th IASTED International Multi-Conference of Computers and Advanced Technology in Education (CATE 2002), Cancun, Mexico*).
Zhang, W., Wang, X., & Khan, M. K. (2015). A virtual bridge certificate authority-based cross-domain authentication mechanism for distributed collaborative manufacturing systems. *Security and Communication Networks, 8*(6), 937-951.

APPENDIX (A)

Information Security Questionnaire for A Comprehensive University IS Security (UISS) Framework For The Protection Of Universities Information Systems

Please give us your insight.

This questionnaire is designed by the student Abdulrhman Ahmed Abdulrazaq for the purpose of the master thesis titled "A Comprehensive University IS Security (UISS) Framework For The Protection Of Universities Information Systems" to fulfill the master degree in computer science.

The questionnaire is exploring the level of information security across the system's departments on University's. Some of the questions may read as if we are trying to catch you out, but we are acutely trying know the level of the security awareness in Al University's system.

Kindly, answer all the questions carefully. We will be grateful for your honest insight, and please remember, these data will serve an educational purpose and your individual responses will remain confidential.

Contact Info:

- Email: aamm240@gmail.com
- Mobile: +966500149921

THE RESPONSIBILITIES OF SECURITY:

Information Security is an important part of my work:

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

Who is responsible for information security at University? (select all which apply)

- ☐ IT Services
- ☐ Deputy Registrar's Office
- ☐ Departments that use data
- ☐ Managers and Team Leaders
- ☐ Individual Employees

I have read and understood University Information Security Policy and Regulation Governing Use of Computing Facilities.

- ☐ Yes, I have
- ☐ No, I have not

I have received Information Security awareness training at the University.

- ☐ Yes, I have
- ☐ No, I have not

Does your work involve any of the following information types? (select all which apply).

- ☐ Student IDs or Personal Details
- ☐ Staff IDs or Personal Details
- ☐ Financial Information
- ☐ Research Information
- ☐ None of the above

Cloud/Network Security

Are network boundaries protected by firewalls in your university?

- [ ] Yes
- [ ] No

Is wireless access allowed in your organization?

- [ ] Yes
- [ ] No

Are employees required to use a VPN when accessing the organization's systems from all remote locations?

- [ ] Yes
- [ ] No

Regular network vulnerability scanning is required.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are required for my organization.

IDS: is a device or software application that monitors a network or systems for malicious activity or policy violations

IPS: is a preemptive approach to network security used to identify potential threats and respond to them swiftly.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral

- [ ] Agree
- [ ] Strongly Agree

Antivirus software must be installed on data processing servers.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Antivirus software must be installed on workstations.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

System Security

Computer systems (servers) must backed up according to a regular schedule.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Servers must be configured in a way to capture who accessed a system and what changes were made?

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

It is a good idea if the organization store backups offsite.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

The organization needs to encrypt its backups.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

The back-up and recovery process must be verified.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Web Security SQL Injection

SQL: Injection is a type of injection or attack in a Web application, in which the attacker provides Structured Query Language (SQL) code to a user input box of a Web form to gain unauthorized and unlimited access.

Organization's website must have confidentiality which could be viewed by unauthorized users.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Organization's website must have integrity to prevent external source to make unauthorized modifications such as altering or even deleting information from target databases.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Organization's website provides authentication to validate user names and passwords.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Organization's website provides authorization to prevent attacker to change authorization information.

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

COMPUTER USAGE

I know what constitutes the use of my computer acceptable

- [ ] Yes, I do know
- [ ] No, I do not know

What I do on my computer could affect other people

- [ ] Strongly Disagree
- [ ] Disagree
- [ ] Neutral
- [ ] Agree
- [ ] Strongly Agree

Passwords are important for preventing unauthorized access to information.

Which of the following are strong passwords according to the University Information Security Policy? (select all which apply)

- [ ] Administrator
- [ ] $ekmoT3bt
- [ ] %2Mst
- [ ] Ahmed
- [ ] secret11

When leaving for lunch or to take a break, how do you secure your computer?

- [ ] I turn my monitor off
- [ ] I log off
- [ ] I lock the computer
- [ ] I turn the computer off
- [ ] I have a password protected screensaver
- [ ] None of the above

If someone e-mails you an attachment/link that is not work related, how likely are you to open it?

- [ ] Not likely
- [ ] Possibly, depending on what is being sent
- [ ] Very likely
- [ ] Always

Does your team share logins and passwords?

- [ ] Yes
- [ ] No

Has anyone you know at work asked for your password?

- [ ] Yes and I provided it
- [ ] Yes and refused to provide it
- [ ] No

I save files to my desktop or to my computer's hard drive

- [ ] Always
- [ ] Sometimes
- [ ] Rarely
- [ ] Never
- [ ] I am not sure

HANDLING INFORMATION

You are asked to provide information containing names and contact details to another office. What is an appropriate method for sending this information? (select all which apply)

- ☐ E-mail message
- ☐ Internet cloud service
- ☐ Phone
- ☐ Hand deliver in hard copy or on USB
- ☐ Internal mail

Electronic and paper documents may contain sensitive personal information e.g. names, pay grades, user codes, addresses etc. Which statement best describes how these documents are handled in your team?

- ☐ Documents are not handled in any special manner
- ☐ Documents are subject to internal procedures and policies to protect confidentiality

How often do you take information home to work on with your home computer?

- ☐ Almost every day
- ☐ At least once a week
- ☐ At least once a month
- ☐ Never

How often do you access University shared drives, files, applications or your emails remotely?

- ☐ Almost every day
- ☐ At least once a week
- ☐ At least once a month
- ☐ Never

I can play a significant role in protecting my computer and the information stored on it

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

There is nothing on my work computer or in my immediate workspace that would

be of any interest or value to others

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

ABOUT YOU

My age:

_____ _____

Gender:

- ☐ Male
- ☐ Female

My position is:

- ☐ Primarily academic
- ☐ Primarily administrative

Which of the following title comes closest to describing your role?

- ☐ Team member
- ☐ Team leader
- ☐ Senior manager
- ☐ Lecturer
- ☐ Researcher

How many years have you worked at the University?

- ☐ Less than a year
- ☐ Between one and three years
- ☐ More than three years

Department/Centre/Unit

_____ _____