# CHAPTER I

## 1.1 INTRODUCTION

E-learning refers to "electronic learning" where in 1990 it was used not as a type of learning, but it was a practice in teaching, design, education and research. Briefly, it is referring to the usage of technology in education and learning. It was adapted on the basis e-learning and the science of instruction-learning should promote psychological engagement between the learner and the lesson content in ways that help learners to select, integrate, and retrieve new knowledge. Also e-learning in the 21st Century is the unique ability to bring together a community of learners, unrestricted by time or place. In present, e-learning can be defined as the use of Information and Communication Technologies (ICTs) to facilitate and enhance learning and teaching. Likewise there are many terms to define this mode of learning and teaching (Friesen, 2009).

The access to information increased dramatically depending on the technology, which facilitated the growing of e-learning, as well as decreasing the cost. The main attribute of ICT is offering the learners a flexible access to information and resources, therefore, it created a suitable environment to individual learners rather than teachers and organizations, which encourage many of them to adopt e-learning (Naidu, 2003).

E-learning is "the term a wide range of uses and processes, for example, learning, and learning based on the computer on the Internet, virtual classrooms, and computerized

cooperation. It includes content delivery by means of the Internet, intranet/ extranet (LAN/ WAN) sound recordings and videos, video, and show television, and web sites on the net, and interactive television, CD ROM, and more than that" (Singh et al., 2005).

Therefore, the definition of e-learning can be as follows: the expansion of the concept of teaching and learning process to go beyond the walls of the traditional classroom sense beyond the conventional method for teaching face-to-face and off for a rich environment for their sources and multiple types of distance interactive technologies and learning a key role where even recast the role of the teacher and the learner, and e-learning does not mean a substitute for the teacher, but since it promotes assisted cycle and as an issue for the brief and orderly organization of the educational process and is compatible with developments in the modern era (Kigozi et al., 2012).

Security is essential as a means to retain users' trust in the web learning environment in light of the fact that any danger can significantly influence students' impression of the system's unwavering quality and reliability. Subsequently, it is significant to distinguish the hidden variables that can bring about security issues in internet learning and to recognize the confinements of the present security assurance techniques. At that point, counter-measures can be produced to relieve the security dangers characteristic in web learning (Chen & He, 2013).

Information security risk in E-Learning system is a topic that has become increasingly significant in the new era especially at schools, universities, colleges and other learning foundations. A data security danger is characterized as any conceivable dangers that

utilization helplessness in the arrangement of an association to bring about disturbance to the authoritative schedules and procedures in some or the other structure. The threats are able to lead to a loss of any form to an individual or an organization. For example, such losses can be included loss of privacy, identity theft, financial loss, negative impact on customer relations, loss or damage of confidential data or information, or a loss in profitability (Beng, 2011).

## 1.2 RESEARCH MOTIVATION

Education is one of the basic pillars upon which in the state is built. In the recent time, e-learning becomes one of the most interesting trends in computer science. It is based on Information and Communication Technologies (ICT) and provides integrated learning service at anytime and anyplace. To ensure the qualities of e-learning system, it must be protected from threats and security risks. Information system security is not only the purpose of the protection of information security assets, but it is also necessary to maintain the security in daily operation process of information system. The research also focuses on the information security risk assessment of e-learning system in Global Open Access Learning System (G.O.A.L.S) in Universiti Sains Islam Malaysia (USIM) aiming at helping system developers to eliminate or mitigate these attacks by identifying the potential vulnerabilities.

## 1.3 BACKGROUND OF THE RESEARCH

Data security is the insurance of data from an extensive variety of dangers with a specific end goal to guarantee business continuity, to minimize business risk and to accordingly maximize return on investments and business opportunities. The objective

is mainly concerned with detecting and preventing unauthorized acts of computer users (Alwi & Fan, 2010).

The significance of data security in the E-Learning environment is that it is essentially reliant on Information and Communication Technologies (ICTs). However, the utilization of ICT could rise numerous conceivable data security risks that could damage and compromise many valuable information. Moreover, these data security risks are not necessary significant in e-learning environment but it also can appear at anyplace. Therefore, all necessary and precaution steps should be taken by educational institutions in order to ensure information is properly and highly secured within the e-learning environment (Beng, 2011).

With the advancement of Information and Communications Technologies and increasing accessibility to the Internet, Institutions become vulnerable to both insiders and outsiders threats. A danger is a portrayal of a potential undesirable occurrence. Data systems are continually presented to different sorts of threats, and these threats can bring about distinctive sorts of harms, which might lead to significant financial losses. Sizes of these harms can extend from little lapses, which just damage the trustworthiness of databases, integrity, confidentiality, availability, to those that devastate entire Computer centers. Thus protecting assets from these threats becomes a major concern for toward both people and Organizations. Dangers originate from distinctive sources, for example, employees' activities, mistakes in data entry or hacker's attacks (Alhabeeb et al., 2010).

Risk assessments have become a standard practice by which organizations determine and demonstrate their privacy, security, and compliance with different strategies that secure against loss. Typical risk assessments include five steps: system characterization, threat assessment, vulnerability analysis, impact analysis, and risk determination. The organizations use the results of a risk assessment in deciding how to apply scarce resources to protect their most important assets (Kaliski & Pauley, 2010).

## 1.4 PROBLEM STATEMENT

Information deriving from useful data has become the main asset in an organization. Nevertheless, when it is always easy for everyone to access, it will also be easy and useful for everyone to gain access. As a result of this increasing intention, it has exposed to a growing number and wider variety of threats and vulnerabilities. Therefore, information security is a crucial factor in the success of an organization. According to Tan (2011), the information should be always being appropriately protected in whatever forms the information takes by which it is shared. Ahmed et al. (2011) clarified that, with the consideration to Information Communication and Technology (ICT), the data to be protected may exist in numerous forms, for instance, it can be in printed form, written down or stored electronically. Whatever forms the data exist, they must be always protected.

Information security also plays vital role in higher education sector as e-learning has become more popular nowadays. Alwi and Fan (2010) mentioned that information security is needed in the e-learning. Pocatilu and Vetrici (2010) explained that online

learning brings with it all of the security risks inherent to the use of the Internet. Therefore, to prevent possible security breaches in online learning, a learning institution should know what are the threats and vulnerabilities that can exploited by unauthorized parties. Jouini and Aissa (2014) clarified that problem arise when there is failure in information security because information worth of billion dollars and high sensitive information are lost every year due to cyber terrorism that has come a way to destroy the world in just a seconds, Nevertheless, learning institution such as universities, colleges, academy, polytechnics are not exception to this kind of attack, that is why a strict information security risk assessment is needed.

This lead to the research problem surrounding the information security in Global Open Access Learning System (GOALS), which is the e-learning system in Universiti Sains Islam Malaysia (USIM). This research will investigate how much damage that resulted from such risks, the level of the threats to the system and ways to curb such occurrences. Institution need to confront the reality to protect sensitive data which is much sensitive in the progress of academies and otherwise. Therefore, researcher will conduct the research entitled "Information security risk assessment of e-learning system: A case study of Global Open Access Learning Systems (GOALS) in Universiti Sains Islam Malaysia (USIM)."

## 1.5 RESEARCH QUESTIONS

RQ1: What are the information security threats faced by GOALS in USIM?

RQ2: How to conduct information security risk assessment for GOALS in USIM?

RQ3: What are the remedies for information security threats faced by GOALS in USIM?

## 1.6 RESEARCH OBJECTIVES

RO1: To identify the information security threats faced by GOALS in USIM.

RO2: To conduct information security risk assessment for GOALS in USIM.

RO3: To propose remedies for information security threats faced by GOALS in USIM.

## 1.7 SCOPE

This study will assess the threats and risks to the e-learning system, and also vulnerability that are been exploited by an unauthorized users. It also provide recommendations that will maximize the protection of confidentiality, integrity and availability, while still providing the functionality and usability of information. The following steps listed below will be use as guidelines; (1) To determine if the risk is intentional or unintentional, (2) To evaluate the risk and decide on precautions, (3) Record the findings and implement them, (4) Review the assessment and update if necessary. The study will carry out information security risk assessment of e-learning systems on a minimum requirement basis based on publications published from 2001 to 2014, and also by collecting data through questionnaires from staff in GOALS. The information security risk assessment of e-learning system aimed at helping system developers in the GOALS at USIM, by identifying the potential vulnerabilities encountered with the information security risk assessment of e-learning system.

## 1.8 DEFINITION OF TERMS

### 1.8.1 E-learning

E-learning can be defined as the use of multimedia technologies which are basically depending on internet in order to improve the teaching and learning quality. Such technique makes accessing to resources, delivering material, and supporting teaching easier. Simply and broadly, it can be defined as learning through Information and Communication Technologies (ICT). E-learning is also known and described by other terms including [online-learning, virtual learning, distributed learning, network and web-based learning]. Moreover, the letter "E" in e-learning refers to (electronic) which means the use of electronic devices (Violettas et al., 2013).

### 1.8.2 Information Security

The aim of information security is to ensure business continuity and minimize business damage by limiting the impact of security incidents (Von Solms & Van Niekerk, 2013).

### 1.8.3 Information Security Risks

Information security risks often emerge because potential security threats are identified that could exploit vulnerabilities in an information asset or group of assets and therefore cause harm to an organization. Having an Information Security System implemented in an organization, does not mean that the organization's assets are protected because the technology is renewable which means that there might be new risks and threats that cannot be detected by an old system. So, in order to have the most secured environment, the organization should conduct what is known by risk analysis (Altamimi, 2011).

### 1.8.4 Risk Assessments

Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk (Rausand, 2013).

### 1.8.5 Risk Analysis

Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that have been identified and to estimate the level of risk. Risk analysis results are used to carry out risk evaluations and to make risk treatment decisions. How detailed your risk analysis ought to be will depend upon the risk, the purpose of the analysis, the information you have, and the resources available. Risk analysis is the basis of information protection, risk management, and risk in the process of information protection (Behnia, et al., 2012).

### 1.8.6 Computer Security

Computer security can be defined in a simple way as: providing a safety to a computerized information system to achieve the perfect and appropriate preservation of the integrity, availability and confidentiality of data including: [hardware, software, firmware, data, and telecommunications). The computer security is applied to secure devices such as computers and computer networks (private and public networks). Thus, this term, includes the processes that protect all the digital equipment, information and services from accidental or unofficial access. Computer security is importantly growing as most societies are dependence on computer systems (Hsiao et al., 2014).

## 1.9 METHODOLOGY

Different kind of methods have been employed in order to test the proposed objectives in regards to Information Security Risk Assessment of E-learning System. Fundamentally, the principle data that have been used in the research were categorized into two main types including: (1) Firstly, previous studies such as books and electronic books, related literature, relevant newspapers and magazines, electronic publication (web pages), and quantitative information to support this research study. (2) Secondly, collecting data throughout employing a questionnaire to Global Online Access Learning System (GOALS) staff to answer questions regarding the Information Security Risk Assessment of E-learning System. Quantitative method was adopted and data gathered were documented for further statistical analyses. This quantitative data allowed a better understanding of how much the Information Security Risk Assessment of E-learning System.

## 1.10 LIMITATION OF THE RESEARCH

Research objectives provided in this study have been achieved by conducting literature review and data collection through questionnaire. But there are some unavoidable limitations such as; the study time was very limited and therefore only one system that is Global Open Access Learning System (GOALS) of Universiti Sains Islam Malaysia (USIM) can be covered for this study.

## 1.11 SUMMARY

Institution must provide adequate protection for their information assets. Information security and risk levels must be well-established at the management level and based on risk assessments. The management of the institution need to confront the reality to protect sensitive data, as well as to carry out information security risk assessment of the data, which is much sensitive in the progress of academics. Enact reforms that honor their core values and remain conscious of the way a university works, while aiming for systematic changes to confidentiality and integrity of information with in the perimeter of the university by carry out information security risk assessment.