A Model for Information Security in e-Learning Management Systems

Prof SH (Basie) von Solms
University of Johannesburg
PO Box 524, Aucklandpark, 2006, Johannesburg, South Africa
basievs@uj.ac.za

Abstract: This paper argues that by ignoring the concept of information security in e-Learning Management Systems (e-LMSs), educational institutions run a very big risk. Such ignorance can have serious consequences for the academic standard of the institution as well as its integrity and the brand name (image).

Executive Management from any academic institution using an e-LMS, must ensure that proper Information Security Governance is enforced – this is an essential component of good Corporate Government.

The paper will present a model (plan) which can be used to evaluate the information security capabilities of an e-LMS.

1. Introduction

Information Security has become core to many, if not all IT systems – with special importance to systems using the Internet as a delivery medium. This fact is well realized and well appreciated in financial systems – specifically Internet based banking systems. What is not so well realized and appreciated is that information security is as important to IT systems supporting e-learning in some way, with special emphasis on e-Learning Management Systems (e-LMSs).

Ignoring the concept of information security in e-Learning Management Systems (e-LMSs) can have serious consequences for educational institutions. Such ignorance can play havoc with the academic standard of the institution as well as its integrity and brand name (image).

It is therefore extremely important to be able to evaluate the information security functionality of an e-LMS.

In this paper we intend to map 6 very important Information Security services to some core actions happening in any e-LMS. This will allow us to understand the role of information security in e-LMS, clearly identify the relevant risks, and help to determine the information security capabilities of an e-LMS.

We start off in paragraph 2 by having a brief look at Information Security Governance Paragraph 3 briefly discusses the 6 essential information security services (pillars) which must be enforced to ensure a secure environment.

In paragraph 4 we describe a typical scenario where IT is tightly integrated in the
educational, teaching and assessment process, and also evaluates the risks involved with the scenario, with reference to the 6 essential information security services.

Paragraph 5 provides a high level approach to evaluate the information security capabilities of an e-LMS, and paragraph 6 provides a final summary.

2. Information Security Governance (ISG)

One general definition of Information Security Governance is:

‘Information Security Governance consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the confidentiality, integrity and availability (CIA) of the company’s electronic assets (data, information, software, hardware, people etc) are maintained at all times’. (von Solms)

From this definition it is clear that in general, the main purpose of ISG is to protect against the risks which can impact on the confidentiality, integrity and availability of all electronic resources. In most cases where information is processed using IT systems, this means the protection of data and information stored in databases and transmitted over networks. This is of course also just as important for educational institutions, where IT is used for such information processing, and where risks can arise against the confidentiality, integrity and availability of the following types of data and information, usually stored in centralized databases:

- student information like course marks and study records
- staff information like salaries and pension information
- intellectual property
- etc

All educational institutions must therefore enforce ISG, at least to protect and secure the types of sensitive information and data referred to above. In most cases, it can be accepted that Executive Management of such institutions are aware of the information security risks as far as these centralized systems are concerned, and that the necessary information security counter measures are installed to manage such risks.

Many educational institutions, however, use IT wider than for just such ‘normal’ information processing. Such wider use includes environments where IT is tightly integrated with the education, teaching and assessment activities, even moving towards a sort of virtual (cyber) based educational environment. One of the main instruments to achieve this, is an e-Learning Management System (e-LMS).

The question is if there are any other risks which can arise in educational institutions where IT is used in this wider sense – risks which are not necessarily present in the more traditional environment. The answer to this question will determine whether Executive Management of educational institutions using e-LMSs, has extra information security governance responsibilities, not necessarily present in cases where only the ‘normal’ and traditional types of information processing is taking place.

In this paper it is argued that such other risks do arise, and if not properly managed
and controlled, can eventually be disastrous for the educational institution.

3. The 6 Pillars of Information Security

The following 6 services must be enforced in all cases to ensure a secure information environment:

Identification and Authentication

This service ensures that only ‘legal’ users, i.e., people who have the right of access to the electronic resources, and who had been properly identified and authenticated as such, can have access to the electronic resources.

Authorization (Logical Access Control)

This service ensures that properly identified and authenticated users can only have access to those electronic resources for which they are authorized.

Confidentiality

This service ensures that all information stored in databases and/or transmitted over networks, can only be read by properly authorized users.

Integrity

This service ensures that all information stored in databases and/or transmitted over networks, can only be changed by properly authorized users.

Non-repudiation/Non-denial

This service ensures that any user who performs any electronic transaction cannot deny having done so.

Availability

This service ensures that all electronic resources and services are available to authorized users when such users want to use such services.

4. A Typical Scenario

Let us envisage the following scenario, not uncommon to many already found in educational institutions, where an e-LMS is used to provide a comprehensive educational and learning management system, allowing students to access such a system, even from remote access points.

The e-LMS allows lecturers (L) and students (S) to perform many transactions, including the following:

- (L) : Load course material onto course websites for students to retrieve
- (S) : Retrieve course material and lectures from a course website
- (S) : Submit assignments to a course website from where lecturers retrieve and mark such assignments
- (L) : Store assignment marks on course website
- (S) : Access a course website to retrieve their marks for assignments
- (L) : Store tests to be written directly on the course website
- (S) : Write difference types of tests directly on their work stations (from different decentralized locations) with results marked by the system and stored on a course database
- (S) : Access course web sites to get the results of tests

Risks which can arise from the scenarios mentioned above, without proper information security governance, include:
- Course material may be altered by unauthorized people
- Bogus course material may be loaded on course websites, or websites may be defaced
- Submitted assignments can be copied from course websites by unauthorized parties
- Submitted assignments can be changed or deleted by unauthorized parties
- Marks can be changed/deleted
- Access to test papers may happen, test contents can be changed, or the test can be deleted before the scheduled test date
- People may masquerade as students and write tests on behalf of such students
- Students may get unauthorized help during the writing of test
- The destruction of course websites and course databases containing marks
- Denial of service attempts against course websites preventing authorized students to access the web site
- Logon information (student/user ID and passwords) of lecturers and students can be intercepted and misused

Let us investigate some in more detail, determine which risks can arise, and indicate which of the 6 information security services are not properly enforced, allowing the risks to materialize.

Suppose a student writes a test from a distributed location, which may be quite an acceptable scenario. Without proper information security governance, the following are some of the problems which may occur:

- Risk: It may not be the ‘correct’ student writing the test. The student might have given his/her student-id and password to another student, who writes the test on behalf of the ‘real’ student. If this is not prevented right at the logon phase, it may probably never be found out
  Reason: Identification and Authentication not properly enforced

- Risk: The answers are intercepted by another student while these answers are being sent over the network, and the interceptor may now submit these answers directly as his/her own
  Reason: Confidentiality not properly enforced

- Risk: During the writing of the test, a student may realize that he/she will not be able to pass the test, and then cause a denial of service attack which may take the web site down, in effect causing the test to be rescheduled because no other student would be able to access the relevant web site anymore
  Reason: Availability not properly enforced

- Risk: A student may log on, but not submit any answers. At a later stage the student may claim that he/she had supplied all answers, and claim that the ‘system lost them’
  Reason: Identification and Authentication, Non-repudiation and Availability (Backups) not properly enforced

- Risk: After a student actually wrote such a test, and found out that she failed, she may claim that she actually never wrote the test, and that some unauthorized person logged in under her name without her consent
  Reason: Non-repudiation not properly enforced

- Risk: A peer to peer wireless network (or even wired network) can
be established between two or more students (or a student and an outside expert), who may then first have a ‘conference call’ amongst themselves to determine the correct answers, and then submit that individually.

Reason: Authorization not properly enforced

Often people reason that such sophisticated actions cannot be performed by ‘ordinary’ students. Do not be misled – there are students who will quickly identify the security weaknesses in the system, with or without specialized help, and exploit and misuse them.

Several other situations can be envisaged based on the scenario above, and all will result in totally unacceptable academic practices.

All teachers and lecturers will agree that such ‘consequences may be too ghastly to contemplate’!

It should be clear that the continuous exploitation of these risks will cause serious academic problems and inconsistencies, the most important of which are that students will be able to get credit for work which they have not done personally and therefore for knowledge which they do not really possess. This will directly lower the standard of the institution and impact on its brand name.

We will now provide a high level approach which can be used to evaluate the information security capabilities on an e-LMS.

5. A High level model (approach) for determining the Information Security capabilities of an e-LMSs

In evaluating the information security capabilities of an e-LMS, it must be determined how well these 6 Information Security services are implemented by the relevant e-LMS.

The following approach can be followed:

1. Perform a risk analysis to determine the scenarios to be implemented through the e-LMS (see paragraph 4 above as examples)
2. Determine the potential risks which can arise from these scenarios
3. Determine which of the 6 Information Security services are needed to address (eliminate) the risks
4. Determine how well these specific Information Security services are implemented by the e-LMS under evaluation.

6. Summary

The idea of using IT and specifically e-LMSs to create and support and a comprehensive educational and learning environment, looks extremely tempting, and can provide major benefits to the relevant academic institution. Many such institutions have therefore already advanced far along this route.

What this paper is warning about, is that if information security governance is not properly enforced in such an environment, the long term consequences may seriously damage the institution. Academic standards will fall, and the problem is that is may not be noticed in the short time. Students exploiting the information security weaknesses in the system, will misuse the systems to their benefits, which will result in the academic standard and (brand) name of
the institution being questions by potential employers. 
By the time top management realizes this, it may be too late to save what is lost.

Top management of educational institutions, using or intending to use IT to provide platforms for integrated educational, learning and assessment environments must understand and accept their Corporate Governance responsibility and accountability for decisions to implement and use such systems.

If they do not, such systems will come back to haunt them.

References