Information security drivers for e-Learning Management Systems (e-LMS)

Sorene Assefa, Prof Basie Von Solms *

Academy for Information Technology, University of Johannesburg, PO Box 524, Auckland Park, Johannesburg, 2006 South Africa

KEY WORDS

E-learning;
E-Learning Management Systems;
Information security;
Information Security Governance;
Information security Policies and Procedures;
User awareness;
Monitoring;
Technical dimension,
Information security services.

ABSTRACT

E-Learning Management Systems (e-LMSs) do provide some form of technical counter measures like password based identification and authentication to protect the valuable system's information assets. Having only technical information security counter measures in place don't necessarily ensure the security of e-LMS environment is maintained at all times. Therefore, information should be taken as multi-dimensional discipline. This article identifies and discusses the most important information security dimensions for creating a secure e-LMS environment.

1. INTRODUCTION

One of the knowledge sharing systems that emerged from the use of Information and Communication Technologies (ICTs) is an e-Learning Management System (e-LMS). An e-LMS is a comprehensive software package with various functional features that enables the management and delivery of online content to remote users via ICT [5].

The integrated and dynamic nature of e-LMS should make it clear that information security is one of the most important aspects to be considered during the implementation and usage of an e-LMS. Moreover, the fact that e-LMSs rely on ICT make it vulnerable to further information security risks. Information security is all about the implementation of information security counter measures to protect a system's information assets from a wide range of threats [2]. Installing antivirus or settings up a firewall are an example of information security counter measures.

* Corresponding author at: University of Johannesburg, PO Box 524, Auckland Park, Johannesburg, 2006 South Africa.. Tel.: +27 11 559 2843; fax: +27 11 559 2138.

E-mail addresses:
soreneas@yahoo.com/200605244@student.uj.ac.za (Sorene Assefa), basievs@uj.ac.za (Prof von Solms).

This article originated from the realisation that the information security is a multi dimensional disciple [6]. Therefore, it is guided by the following question. *Which information security dimensions are most relevant in creating a secure e-LMS environment?*

The authors identified the five most important information security dimensions that should be put in place to enhance the overall information security of an e-LMS environment.

2. THE FIVE INFORMATION SECURITY DIMENSIONS

The five information security dimensions for e-LMSs are:

- The e-LMS Information Security Governance(ISG) Dimension;
- The e-LMS Information Security Policies and Procedures Dimension;
- The User Awareness Dimension;
- The Monitoring Dimension; and
- The Technical Dimension;

These information security dimensions and their respective action(s) will be discussed further.

2.1. The e-LMS Information Security Governance(ISG) Dimension

The main goal of Information Security Governance (ISG) is to develop information security goals and objectives for an e-LMS [7]. It is therefore necessary to introduce and ensure information security measures are implemented to make sure the security objectives of the e-LMS are achieved.

2.2. The e-LMS Information Security Policies and Procedures Dimension

The information security Policy and Procedure dimension is one of the most important information security dimensions. Information Security Policies and Procedures can be defined as the document that addresses "what must be managed" and "how this should be done" regarding e-LMS information security [4 and 6]. Therefore, the Policy and Procedure Dimension serves as a guideline which deals solely with the policies and procedures that must be in place in order to manage and enforce information security. For instance, a password policy is a guideline for the end users to follow during the creation and usage of passwords. Some of the most common elements of a password policy are:

- The minimum length of password allowed by the system.

- What kind of characters should be allowed in order to form a password?
- How frequently the passwords should change.

2.3. The User Awareness Dimension

The User Awareness Dimension deals with creating an information security awareness program for end users [1 and 6]. User awareness programs should focus on creating an acceptable level of awareness of information security policies and procedures created for the e-LMS, as well as the users' roles in maintaining the information security of the e-LMS. Having technical information security measures by itself do not ensure information security; it is necessary that end users are aware of it and act in a way that does not compromise the technical measures. For instance, if the e-LMS uses password based information security mechanisms to implement identification and authentication services and the user gives out his/her password intentionally or unintentionally (i.e. posts his/her password on his/her table), the whole information security measure is compromised. Therefore, an information security awareness program is a vital control in securing the e-LMS environment [1].

2.4. The Monitoring Dimension

The aim of the Monitoring Dimension is to define a monitoring mechanism that will be used to determine the performance of the information security mechanism, which has been implemented to mitigate or reduce the information security risks to an acceptable level.

2.5. The Technical Dimension

Information security can be defined as the establishment and maintenance of controls and measures aimed at minimizing the risk of loss, disclosure, corruption, and disruption of access of information resources [3]. From this definition it is clear that the main purpose of information security is to protect and ensure that the authorization, confidentiality, integrity, and availability of information resources are maintained at all times.

The Technical Dimension ensures the six information security services that are necessary to enhance the information security of the e-LMS environment are enforced. The six information services are identification and authentication, authorization, confidentiality, integrity, non denial and availability.

There is no fixed boundary between these dimensions and should be treated in a harmonized way. In the next section, the interdependency of the five information security dimensions will be discussed in detail.

3. THE INTER-RELIANT OF THE FIVE INFORMATION SECURITY DIMENSIONS

The scenario below illustrates how necessary the five information security dimensions are in enforce an effective identification and authentication information security service in an e-LMS environment.

- ✓ 'Bob', the system administrator, has decided to use a password based mechanism (i.e. the technical dimension). To create a strong identification and authentication, Bob creates password police and procedures that needs to follow by users during the creation of an identity (username/ password) as well as utilizing the mechanism (i.e. the policy and procedure dimension). Bob decides to create an information security awareness program so that end users are aware of the information security policies and procedures and act in a way that does not compromise the technical measures (i.e. the user awareness dimension). Bob wants to make sure that the information security mechanism implemented has served its objectives (i.e. the monitoring dimension). Bob agrees to ensure the Information Security Governance (ISG) is implemented throughout the e-LMS environment.

As has been noted from the scenario above, to create and maintain a secure e-LMS environment it is necessary to take all the five information security dimensions into account.

4. CONCLUSION

In this article, the five most important information security dimensions that need to be considered in creating a secure e-LMS environment have identified. Moreover, it stresses the fact that each of the five

information security dimensions are equally important and it is necessary to take all these dimensions into account to implement and maintain the information security of an e-LMS environment.

ACKNOWLEDGMENT

We would like to thank the National Research Foundation (NRF) and University of Johannesburg (UJ) for the financial support.

REFERENCES

[1] Du Plessie, L. and Von Solms, R. (n.d.) Information Security Awareness: Baseline Educator and Certification. Port Elizabeth technikon

[2] Grobler, T. and Louwrens, B. (n.d.). "New Information Security Architecture". University of Johannesburg

[3] Hone, K. (2004). "The Information Security policy- An important information security management control".

[4] kritzinger, E. and Von Solms, S.H. (2006). "E-Learning: Incorporating Information Security Governances". Issues in Informing Science and Information Technology. Volume 3.

[5] Von Solms, S.H. (2005). *Information security Governance in ICT based educational systems.*

[6] Von Solms, S.H. (2001). "Information Security – A Multidimensional discipline". ElSevier Science Ltd.

[7] Conner, F.W. and Coviello, W.A. (2004). "Information Security Governance – A call to Action". National Cyber Security Summit Task Force.