Information Security in an E-learning Environment

E. Kritzinger
School of Computing, University of South Africa,
PO Box 392, UNISA, 003, South Africa.

Abstract. In the last few years the education environment underwent a paradigm shift due to the rapid growth in technology. This growth made it possible for the education environment to utilize electronic services to enhance their education methods. It is, however, vital that all education environments (traditional or new ones) ensure that all resources (lectures, students and information) are properly protected against any possible security threats. This paper identifies technical and procedural (non-technical) information security countermeasures that could enhance the security of information within the education environments.

1 Introduction

Information security has become a much-discussed subject all over the world in the last few years. All institutions (including educational institutions) should realize that information is an extremely valuable resource and must be protected at all cost. Information security is therefore no longer a luxury, but a necessity in all institutions. A great deal of research has already been conducted in educational environments. However, one aspect that has not received much attention is the important role of *Information Security,* especially in newer education environments such as the e-learning environment. Information must be protected due to the development of newer technologies that could be used in an attempt to compromise the security of information. The first part of this paper focuses primarily on the difference between a traditional educational environment and the e-learning environment in regards to securing information against unauthorized access. The second part of the paper

provides different technical and procedural countermeasures that could be used as guidelines to protect information within the e-learning environment.

2 Traditional educational environment vs. e-learning

Educational institutions use different environments to educate students. This paper will primarily focus on two well-known environments, the traditional environment and the e-learning environment. The rest of this section will provide a brief overview of each environment and investigate to what extent information security is needed within these two education environments.

2.1 Traditional education environment

The traditional education environment (as depicted in Figure 1) has been around for many years and is found all around the globe. This educational environment consists of a central physical teaching facility (institution) which consists of lectures, students and databases. These databases could consist of public as well as sensitive information.

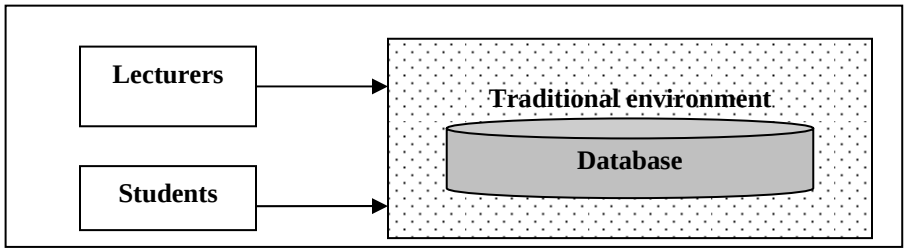

Figure 1. Traditional education environment

Information security is adequately addressed within a traditional environment due to the fact that traditional education environments are mostly restricted to one physical location. This means that lecturers and students as well as the databases are grouped together in a closed system environment where information security threats could be kept to a minimum. For example, all students must identify (ID or student card) themselves before they are admitted to the examination. This ensures that lecturers are certain that the students who are writing the exam are the students who enrolled for that specific course. This will eliminate the possibility that any other person can pretend to be a student and write the examination on behalf of that student.

This changed when educational institutions decided to change their traditional way of education and incorporate newer technologies to be able to provide education electronically over the Internet. This method of education is called e-Learning (electronic learning).

2.2 E-learning environment

E-learning can be defined as technology-based learning in which learning material is delivered electronically to remote learners via a computer network [5]. E-learning (or Internet-based learning) could be seen as a professional level of education but with the advantages of lower time and cost [3]. Some other advantages of e-learning include larger learner population, shortage of qualified training staff and lower cost of campus maintenance, up-to-date information and accessibility [1][3]. In a typical e-learning environment the lecturers, students and information are in different geographical locations (as depicted in Figure 2) and are connected via the Internet.

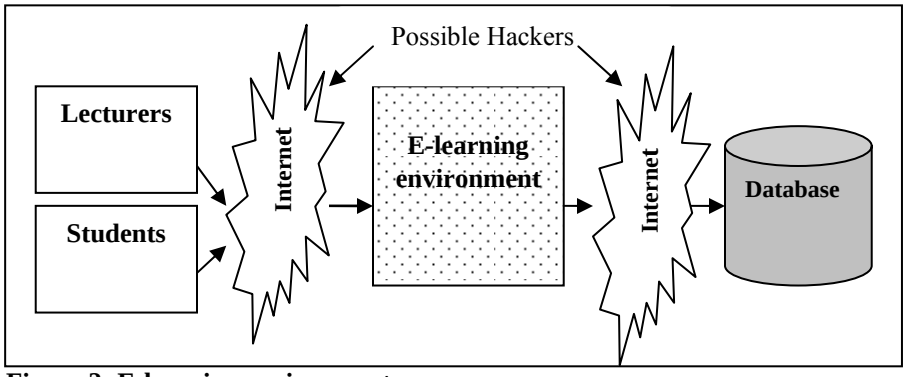

Figure 2: E-learning environment

A lot of research has been done regarding the *advantages* of e-learning. However, not much attention is given to the important role that information security plays within the e-learning environment. Information security is vital for any e-learning environment due to the fact that e-learning is fundamentally dependent on information and communication technologies (ICT). The use of ICT in the e-learning environment opens doors to many possible (information security) risks that could compromise the whole e-learning environment. It is this dependency on the Internet (the lifeline of e-learning) that contributes to the greatest information security risk. Consider some examples where information could be compromised:

- A student could intercept another student's work and resubmit it as his/her own work.
- A student could obtain unauthorized access to the examination marks database and change his/her examination mark, or the marks of any of the other students.
- A student could receive assistance while writing the examination.

These are only a few of the illegal actions that could occur within the e-learning environment if information security measures are not appropriately implemented. These actions could occur due to malicious intent or by plain ignorance on the part of the user on how to properly secure the information they work with. Both of these issues should be addressed before information would be secure.

3 Countermeasure

With the increasing information security threats within the e-learning environment as indicated above, institutions should implement technical as well as procedural information security countermeasures to ensure the availability, integrity and confidentiality of their information.

3.1 Technical countermeasures

According to Von Solms (an international information security specialist) there are six technical countermeasures that should be adhered to when implementing information security within any education environment [4]. Implementing these countermeasures will help to ensure that lecturers and students as well as data (such as student marks and financial information) are properly protected against possible security incidents. These information security countermeasures are:

- *Identification and Authentication* – ensuring that the user is who he/she claims to be and to ensure which access is granted to the user.
- *Authorization* – ensuring that the user has the authority to access the system or information.
- *Confidentiality* – ensuring that information is not disclosed to any unauthorized people.
- *Integrity* – ensuring that the information is unchanged and in its original form.
- Non-repudiation – ensuring that a person cannot take an action that can be denied later on.
- *Availably* – ensuring that the information is available at any given time.

These six information security countermeasures are primarily seen as technical information security countermeasures due to their technical orientation (for example encryption, access control lists and message authentication codes). However, information security is not only a technical issue but a business issue as well. The next subsection investigates different business or procedural information security countermeasures.

3.2 Procedural countermeasures

It is pivotal that information security is not only seen as a technical issue but also as a procedural or a business one. This section provides four procedural information security countermeasures that will address the business side of securing information within e-learning. These countermeasures are:

- Ensure Information Security Governance – Get approval and buy-in from top management who are ultimately responsible for information security.
- Implement an E-learning Information Security Policy - An e-learning information security policy should be used as a guideline to *what* must be managed and *how* this should be done regarding information security.

- Establish an E-learning Security Risk Management Plan - Top management of educational institutions should provide platforms for integrated educational, learning and assessment environments to minimize any possible information security risks and threats.
- Proper Monitoring of Information Security measures - Information security compliance monitoring is about finding out if information security related procedures and processes are implemented and are working as they should.

These countermeasures (technical and procedural) should not only be adopted in the e-learning environment but also be implemented and enforced.

3.3 Identifying stakeholders and assigning roles and responsibilities

In the shift between the traditional and e-learning environments, the roles of lecturers and students have changed. Not only have the roles of some role players changed, but new role players are also emerging. It is therefore vital that institutions identify these stakeholders and ensure that they are properly made aware of their roles and responsibilities towards securing the information they work with.

4 Conclusion

E-learning depends on the Internet, which on its own contributes to many information security threats. It is therefore vital that all e-learning environments should ensure that information security countermeasures (technical and procedural) are properly understood and implemented as well as possible.

References

1. El-Kahatib, K., Korba, L., Xu, Y. & Gee, G. (2003). Pravacy and Security in E-Learning. *International Journal of Distance Education,* 1(4).
2. Katzke, S. (2001). Security Metric. Available at: http://www.acsac.org/measurement/position-papers.
3. Silver, M. (2004). E-Learning for the pump industry. *Worls Pumps,* 2004(453): 28-31.
4. Von Solms, S. H. (2005). Information Security Governance in ICT Based Educational Systems. *Proceedings of the 2005 Conference in Bankok.*
5. Zhang, J., Zhao, L. & Nunamaker, J. F. (2004). Can e-learning replace classroom learning? *Communications of the ACM,* 47(5): 75-79.