E-learning: Incorporating Information Security Governance

E. Kritzinger
University of South Africa, Pretoria, SA
kritze@unisa.ac.za

S.H von Solms
University of Johannesburg, Johannesburg, SA
basie@krw.rau.ac.za

Abstract

The global society is living in the electronic age where electronic transactions such as e-mail, e-banking, e-commerce and e-learning are becoming more and more prominent. This paper primarily focuses on e-learning and how important it is to ensure that proper Information Security measures are put in place to ensure that all information within the e-learning environment is properly protected. This paper highlights four Information Security pillars that could be used to achieve this.

Keywords: electronic learning, e-learning, information security, countermeasures

Introduction

Education methods within the education environment have undergone a paradigm shift of over the last few years. This is primarily due to the introduction of newer and better technologies for example the Internet. One new education method that emerged from using these new technologies is Electronic Learning (E-learning). E-learning can be defined as technology-based learning in which learning material is delivered electronically to remote learners via a computer network (Zhang, Zhao, & Nunamaker, 2004). A great deal of research has already been done in the e-learning environment. However, one aspect that has not received much attention is the important role *Information Security* plays within the e-learning environment.

The primary reason why *Information Security* is so important within the e-learning environment is that e-learning is mainly dependent on information as well as communication technologies (ICT). The use of ICT however, could lead to many possible Information Security risks that could compromise information. These Information Security risks are not necessarily unique to the e-learning environment but should however be addressed as if it where. It is therefore vital that all necessary steps be taken by educational institutions to ensure information is properly secured within the e-learning environment.

Possible Information Security Risks Regarding E-Learning

Let us envisage the following scenario where an e-learning environment allows students to access a system from remote access points. This scenario is not uncommon and many such scenarios could

already be found in educational institutions all around the globe. A comprehensive e-learning environment exists, where lecturers (L) and students (S) can do the following:

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

Please note that the examples above are not the only actions with in e-learning, however it is sufficient enough to illustrate the scenario. Information Security risks that can arise from the above mentioned examples without proper Information Security include the following:

- Course material may be altered by unauthorized people,
- Bogus course material may be loaded on course web sites, or web sites may be defaced,
- Submitted assignments can be copied from course web sites by unauthorized parties,
- Submitted assignments can be changed or deleted by unauthorized parties,
- Marks can be changed/deleted,
- Access to test papers may be gained, 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 tests,
- The destruction of course web sites and course databases containing marks
- Denial of service attempts against course web sites preventing authorized students from accessing the web site.
- Logon information (student/user ID and passwords) of lecturers and students can be intercepted and misused.

The Information Security risks identified above should be addressed by ensuring that the e-learning Information Security countermeasures are implemented thought out the e-learning environment. This paper proposes four e-learning pillars that could help institutions in securing their information against harmful attacks.

E-Learning Information Security Pillars

The four main pillars that the authors claim to be essential for proper Information Security within the e-learning environment are as follows:

- Ensuring e-learning Information Security Governance
- Creating e-learning Information Security Policies and Procedures
- Implementation of e-learning Information Security countermeasures
- Monitoring the e-learning Information Security countermeasures

A combination of these four pillars will have a significant effect on implementing and maintaining a good and secure e-learning environment. These four pillars are depicted in Figure 1.

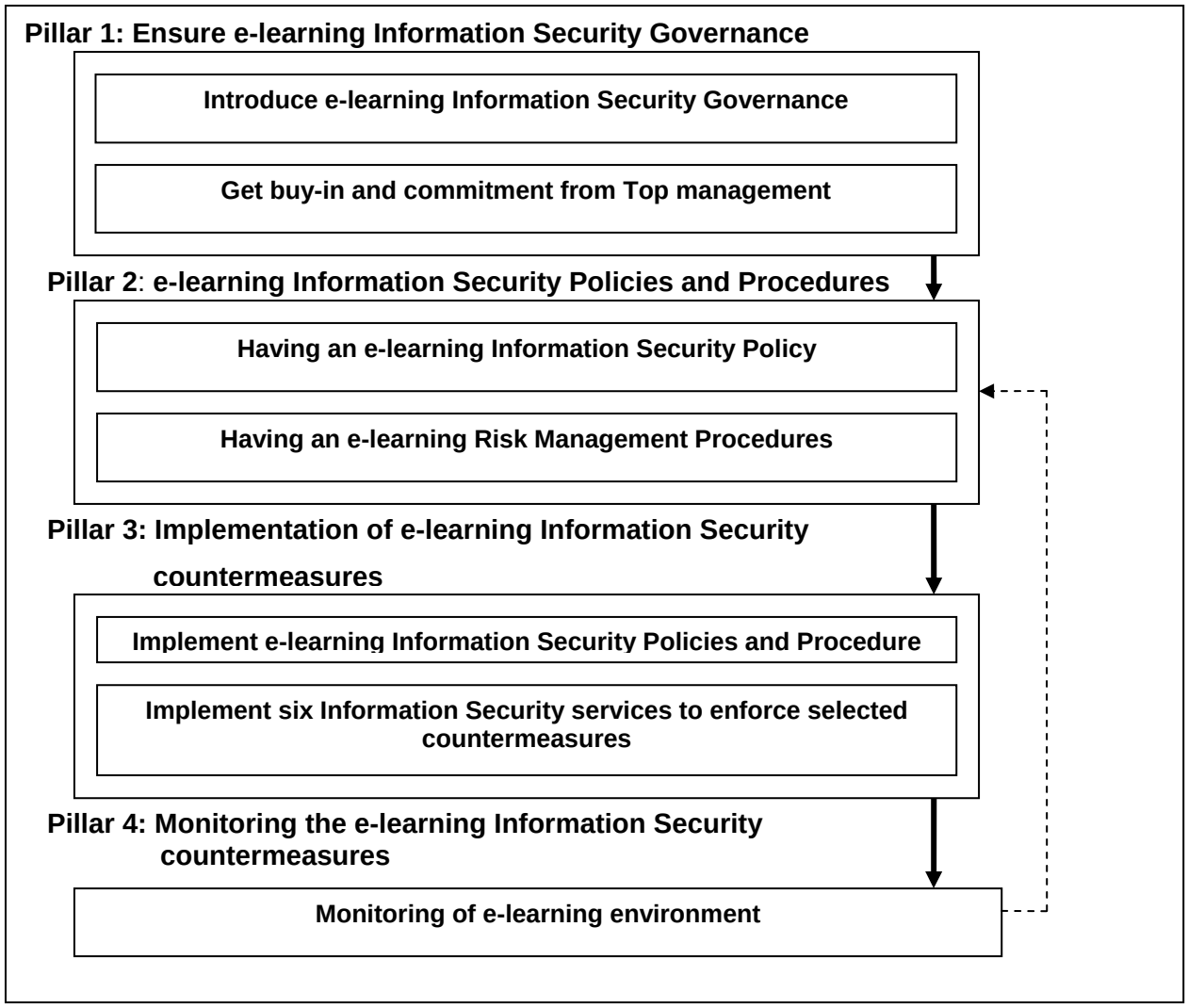

Figure 1: Four Pillars of e-learning

Each of the four pillars consists of one or more actions that will help the institution in implementing that specific pillar. Each of the pillars as well as the actions (depicted in Figure 1) will be separately looked at in the rest of this paper.

Ensuring E-Learning Information Security Governance

The first pillar highlights the significance of Information Security Governance within the e-learning environment and consists of two actions. The first action is to ensure proper Information Security Governance and the second actions is about the buy-in and commitment from Top management.

Introduce e-learning Information Security Governance

Information Security Governance consists of the leadership, organizational structure, processes and technologies that ensure that information is never compromised (Von Solms, 2001b). From this definition it is clear that in general, the main purpose of Information Security Governance is to protect against the risks that can impact on the confidentiality, integrity and availability of all electronic resources. In most cases information is processed using Information and Communications Technologies (ICT) systems, this means the information is stored in databases and transmit-

ted over networks. This is naturally just as important for educational institutions, where ICT is used for such information processing, and where risks can arise with regard to 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 should therefore enforce Information Security Governance, at least to protect and secure the types of sensitive information and data referred to above.

Get buy-in and commitment from top management

The second action in this pillar highlights how important it is to obtain the buy-in and commitment from Top management. Top management is ultimately the responsibly to ensure that Corporate Governance is implemented within the institution. This responsibility is enforced by law in many countries and in many cases Top management can be taken to court and held accountable if the integrity, availability or confidentiality of information is compromised in any way (Lindup, 1996). Top management should therefore protect information through effective management, which is assured only through effective board oversight (Von Solms, 2001a). Only if Top management takes Information Security seriously will the rest of the institution will follow.

E-learning Information Security Policies and Procedures

The second pillar is about ensuring that proper e-learning Information Security policies and procedures are designed and implemented within the institution. This pillar also consists of two actions which include policies and risk management procedures. Both of these actions is vital in ensuring information is secured.

Having an e-learning information security policy

Before any institution can start managing Information Security, they should have an e-learning Information Security policy in place. This e-learning Information Security policy should be used as a guideline as to **what** must be managed and **how** this should be done. An e-learning Information Security policy (like any other policy) should be a document that addresses the rules and regulations regarding e-learning within the institution and should directly relate to the institution's e-learning policy.

This e-learning Information Security policy should address how security decisions can be made with regard to hardware, software, networks and information. The primary purpose of an e-learning Information Security policy is to protect the institution's information assets from all possible threats. Such an e-learning Information Security policy should comprise of a maximum of 2 to 3 pages, very generic, and non-technical, and must be signed by the most senior official in the company.

Having an e-learning risk management procedures

The second action in this pillar is to prevent the Information Security incidents within the e-learning environment. Top management of educational institutions should provide platforms for integrated educational, learning and assessment environments. This could be done by following at least, the following steps:

- Perform a proper risk analysis to identify all the ICT and business-related risks involved in the implemented, or intended, system. Ensure that this risk analysis is driven by international best practices in the field of ICT and Information Security governance.
- Determine the potential impact of these risks on the institution if they should materialize.
- Determine how to handle these risks, i.e. ignore them, transfer them or accept and manage them.
- Determine the Information Security countermeasures needed to manage those risks which are accepted.
- Create a proper Enterprise Information Security Management (EISM) system to continuously manage these risks. Such a system should include the relevant policies, procedures, technical measures as well as the necessary compliance measurement and monitoring mechanisms to monitor and enforce compliance with the relevant policies, and to report the level of risk to top management on a regular basis.
- Review the risk situation on an annual basis and adapt the EISM system as necessary.

Implementation of E-Learning Information Security Countermeasures

The third pillar highlights the implementation of different Information Security countermeasures. This pillar consists of two actions, the first is about the implementation of policies and procedures (see also section 3.2). The second action identifies six countermeasures that are vital for overall security within e-learning.

Implement e-learning information security policies and procedures

It is essential that all institutions ensure that their e-learning Information Security policy is not only properly designed but also properly implemented. An e-learning Information Security policy has no value if it is stored somewhere on a shelf and is not used to secure information. If an e-learning Information Security policy is not implemented within the institution, it is just as bad as not having one at all. However, the implementation of the e-learning Information Security policy however is ultimately the responsibility of Top management.

Implement six information security countermeasures

The second action in this pillar is to identify and implement six Information Security countermeasures. When implementing Information Security countermeasures within the e-learning environment it is essential that the implemented countermeasures should enforce the following six Information Security services:

1. Identification and Authentication. The first service, identification and authentication, is put in place to ensure that only authorized users can gain access to a system (or part of a system). The first part of this service is about determining whether or not a person who is trying to gain access to a system is cleared for access. This process is called identification and is usually done by entering a user ID into the system. Once the user has been identified, the system must ensure that the user is truly who he/she claims to be. This process is called authentication. Authentication can be done by means of something the user knows, such as passwords, something the user has, such as an access card or something the user is, such as fingerprints (Von Solms & Eloff, 2004). Examples of the Information Security countermeasures for identification and authentication include proper unique passwords and login IDs.

2. Authorization. The next step towards enforcing Information Security is authorization. This involves determining whether or not the authenticated party has the right to access the information in question (Von Solms & Eloff, 2004). An example of the Information Security countermeasures for authorization is a*ccesscControl.*

3. Confidentiality. The third service, confidentiality, is an Information Security characteristic as well as a service and is put in place to protect data from unauthorized access. The purpose of confidentiality is to ensure that information and data are not disclosed to any unauthorized person or entity (International Federation of Accountants, 2000). An example for the Information Security countermeasure for confidentiality is *encryption*.

4. **Integrity**. The fourth service is integrity. The purpose of integrity is to ensure that information is still in its original form and that no tampering or alteration has taken place. In other words, only authorized parties may change the content of information and unauthorized modification must be prevented. An example of a countermeasure that will help to ensure integrity is m*essage authentication codes.*

5. **Non-Repudiation**. The last step towards enforcing Information Security is non-repudiation or non-denial. This service ensures that no action taken that affects Information Security can be denied at a later stage (Von Solms & Eloff, 2004). An example of the Information Security countermeasure for non-repudiation *is digital signatures*.

6. **Availability**. This service ensures that all electronic resources and services are available to authorized users when they want to use such services. Availability means that data and information is accessible at any time to authorized parties (International Federation of Accountants, 2000). An example of the Information Security countermeasures for availability is regulator b*ackups*.

Monitoring the E-Learning Information Security Countermeasures

The fourth and last pillar is about Information Security compliance monitoring to establish if procedures and processes that are implemented in an organization are working as they should. The objects that are monitored can differ from organization to organization and include products, systems, processes, security program effectiveness and personal competence (Katzke, 2001). This monitoring process should therefore be extended to include the e-learning environment and include aspects such as validation of information, evaluating of the operating capacity as well as overall impact of the e-learning environment on learners' success.

This monitoring process will ensure that institutions know their Information Security situation within the e-learning environment at any given time. This will also help Top management in their decision making process to ensure that if there is a security incident, it can be resolved before the availability, integrity and confidentiality of information is compromised. If any difficulty is identified by the monitoring process it is essential that the e-learning Information Security policies and Risk Management procedures are updated at regular intervals (as depicted in Figure 1).

Conclusion

This paper highlighted how important it is to ensure that information within the e-learning environment is secured at all times. The authors identified four pillars that should be put in place to enhance the overall Information Security as regards to e-learning. Each of these pillars and its actions should be individually addressed and implemented. However, all four pillars should be seen as a top-down approach that Top management could use for guidelines to ensure that Information is secured within the e-learning environment.

References

Deloitte. (2005)*:* 2005 global security survey. Available at: http://www.deloitte.com

International Federation of Accountants (2000). *Managing security of information*.

Katzke, S. (2001). Security metric. Available at: http://www.acsac.org/measurement/position-papers.

Kwok, L. & Longley, D. (1997). Code of practice: A standard for information security management. In *Proceedings of IFIP TC11, 13th International Conference on Information Security*.

Lindup, K. (1996). The role of information security in corporate governance. *Computers & Security, 15*(6): 477-485.

Von Solms, S. H. (2001a). Information security - A multidimensional discipline. *Computers & Security, 20*(6): 504-508.

Von Solms, S. H. (2001b). Corporate governance and information security. *Computers & Security, 20*(3): 215-218.

Von Solms, S. H. & Eloff, J. H. P. (2004). *Information security*, Johannesburg, South-Africa.

Zhang, J., Zhao, L. & Nunamaker, J. F. (2004). Can e-learning replace classroom learning? *Communications of the ACM, 47*(5): 75-79.