E-Learning and Information Security Management

Najwa Hayaati Mohd Alwi, Ip-Shing Fan
Cranfield University, UK

Abstract

Many e-learning institutions are rushing into adopting ICT without carefully planning and understanding any related security concerns. E-learning is a new method of learning which ultimately depends on the Internet in its execution. The Internet has become the venue for a new set of illegal activities, and the e-learning environment is now exposed to such threats. In this paper, e-learning context, definition, characteristics, development, growth, benefits and challenges are all elaborated upon. This paper discusses the security elements required to be implemented within e-learning environments. In addition, the paper explains the situation and existing research relating to security in e-learning. Furthermore, information security management is suggested to contribute to preparing a secured e-learning environment.

1. Introduction

The growth of Information and Communication Technology (ICT) has significant effects on all people around the world. With this growth, people are able to connect with each other, especially through the Internet. These days, the Internet itself is drastically varying the provisions of services and goods, simply because of its features: immediacy, openness, ubiquity, and global reach. Moreover, e-services have been introduced widely; thus, the education industry has fully detained its new potential as long life learning tools from the Internet features, such as in the form of the web application, for example. This industry is poised to become one of the largest sectors in the world economy.

The development of e-learning has subsequently led to a new way of learning and, at the same time, has given equal opportunities to everyone to become learners. With such methods of learning now available, it is said that information or knowledge can be reached at fingertip level, and thus enable students to excel in their studies. However, despite the Internet as a place to obtain all necessary information and knowledge, it has also become the venue for a new set of illegal activities. Information on the Internet is continuously exposed to security threats. As a consequence of e-learning having to depend on the Internet or, specifically, mostly via web applications, the e-learning environment has also become affected by security threats. With this in consideration, this paper aims to explore the wider context of information security issues and threats, and the potential of information security management in reducing them.

The first part of this paper discusses the e-learning context — the definition, characteristic, development, growth, benefit and the challenges — all of which consider security in e-learning as a new challenge in implementing the e-learning environment. Moreover, web applications are the medium used to aid the majority of online services and, hence, have become the prime target of Internet attacks.

The second part of this paper looks at information security in e-learning which has been neglected in research. Many e-learning institutions are rushing into adopting ICT without carefully planning and understanding the ever-present security concerns. Issues such as legitimate users, course content reliability, and accessibility (including the admissibility and availability), as well as other considerations, all need to be carefully addressed in order to ensure the learning process can effectively take place. Lastly, the paper will discuss the potential of information security management to be implemented in the context of e-learning, in order to prepare a secured e-learning environment.

2. E-Learning

E-learning is the term used to describe the use of the web and other Internet technologies in terms of enhancing the teaching and learning experience. It shares similar characteristics of many other e-services, such e-commerce, e-banking and e-government. The e-services users' behaviours are different according to their roles and needs. E-learning users focus on how to benefit from e-learning concerning teaching and learning purposes. The users may need to spend longer periods of time when undertaking e-learning compared to other e-services.

2.1. Definition and Characteristics

There are many different definitions of e-learning present in the literature, and each one has a different

emphasis: some focus on the content, some on communication, and some on the technology [1]. One of the early definitions for e-learning was provided by the American Society for Training and Development (ASTD), which proposes that e-learning covers a wide set of applications and processes, such as web-based learning, computer-based learning, virtual classrooms, and digitals collaboration.

E-learning is the implementation of technology in order to support the learning process, whereby knowledge or information can be accessed using the communication technology. The learning process can be continuous, provided that the content is available on the net. Eklund [2] defines e-learning as a component of flexible learning, which is a wide set of applications and processes, all of which use all available electronic media to deliver education and training; this includes computer-based learning, web-based learning, virtual classrooms, and digital collaboration.

2.2. E-learning Development and Growth

The use of technology to support learning was started as early as the 1980s. Such a development was also in conjunction with the dissemination of computers for personal use at that time. In fact, higher learning institutions have also dramatically changed over the last thirty years in consideration of policy drivers, such as widening participation, long life learning, and quality assurance [3]. Figure 1 below shows the maturity of e-learning through 1983 until the present day. The emphasis on e-learning in the past has been on the 'e', which refers to electronic or technology. There is an urge to shift to the learning (content) in ensuring the success of e-learning. Moreover, there are some common terms which are used interchangeably so as to reflect the usage of technology in education, such as distributed education, e-learning, distance education, blended learning and online classes.

Distance education relates more to self-learning. In this instance, the learning materials are posted through physical mail or can be accessed online. The meeting sessions are conducted only a few times per semester. Meanwhile, the combination of face-to-face and online learning sessions is referred to as blended learning and are quite popular nowadays.

It is a method of educating at a distance which utilises technology combined with traditional education or training. Strategic learning delivery channels are used, such as physical classrooms, virtual classrooms, print, email and message boards, mentoring systems, software simulations, online collaboration, and mobile and wireless channels [5]. As depicted in Figure 2, Mason and Rennie [1] position e-learning as a type of distance education. They also mention that 'distributed education' is a broader term which includes aspects of distance and online education, as well as being blended with face-to-face learning.

Pre 1983 - Era of Instructor-led Training	This was the dominant teaching tool before computers became widely available, and when interactions between the instructor and students took place in the classrooms.
1984-1993 – Multimedia	Windows 3.1, Macintosh and CD ROMs were the main technology developments during this period. However, classroom interactions and dynamic presentations were lacking in this medium.
1994-2000 – Web Infancy	As the web evolved, the arrival of e-mail, media players and streaming audio/video began to change the face of multimedia mediums. Students were able to access lecture notes or materials from the web at any time and at any (Internet-capable) location.
2001 and beyond – Next-generation Web	Advanced website design, rich streaming media (real audio/video) and high bandwidth (faster data flow) will revolutionise the way in which education will be delivered. Instructor-led, interactive modes can now happen via the web, reaching far more students than before.

Figure 1. The Maturity of E-learning [4]

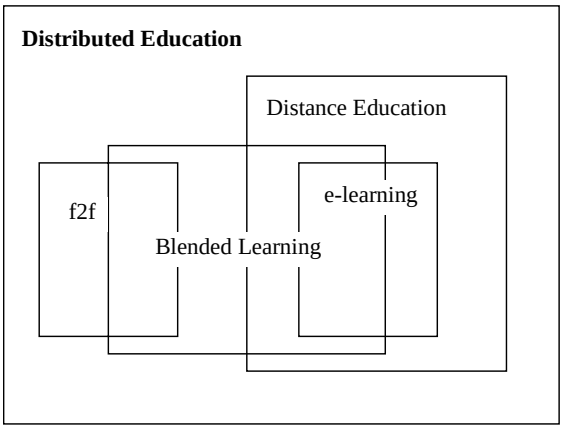

Figure 2: The Relationship of E-learning to Distribution Learning (Mason & Rennie, 2006)

Today, the implementation of e-learning is a combination of three ways of using technology: using technology asynchronously, i.e. only as tools

to support or supplement a traditional (face-to-face) learning, using technology asynchronously and synchronously as tools to support or supplement a traditional (face-to-face) learning, and using technology asynchronously and synchronously to deliver a learning course (completely online). Figure 3 depicts the flow of communication between students and educators in the e-learning system component.

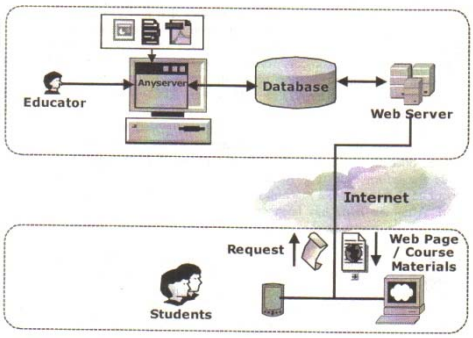

Figure 3: E-Learning Systems Components Diagram (Au *et al*., 2003)

Regardless of the claim that many e-learning initiatives have fallen short of expectations, the market of e-learning is nevertheless continuing to grow. Reports from the Sloan Foundation indicate that 3.5 million students (representing almost 20% of all U.S. higher education students) enrolled in at least one online course during the fall 2007 term [6]. This growth is fuelled by new institutions entering into the online arena, combined with a continuous student demand for online learning options. The need of knowledge workers has also contributed to the growth of e-learning: every employee needs to equip themselves with the knowledge and skills to as great a degree as possible, so that they can progress; the easiest way to do this is to enrol as an e-learning student.

Figure 4: The E-Learning Functionality Growth

The functionally of e-learning has also grown in parallel with the needs and the developments of technology. Figure 4 shows the growth in e-learning functionality. Initially, e-learning publishes the learning content on the Internet, and enables it to be accessible by the user at any time and at any location (asynchronous learning). It then broadens to allow the learning session to be conducted at anytime and anywhere (synchronous learning) from the perspectives of all users (instructor/lecturer and students). E-learning now enables the registration, assessment, and posting graduation certification online. With the intention of adding greater flexibility, mobile learning has been introduced despite the fact that usage is currently limited and not fully utilised. As the functionality of e-learning continues to grow, the e-learning environment needs to become more secured. Greater functionality presented to users will make the e-learning environment more open and exposed to the information security threats.

2.3 Benefits of E-Learning

Nowadays, employees must be able to follow and remain in-line with technological changes and accordingly perform innovative problem-solving. One way of meeting the demand for these new skills, especially in Information Technology, is via e-learning, which also offers the potential for continuous learning.

E-learning offers everyone the opportunity to become a learner. The concept of anytime, anywhere learning promotes life-long learning and accordingly eliminates the problems associated with distance. The flexibilities which e-learning offer to the students is the main motivating factor in choosing online courses [7]. Moreover, the usage of technology in learning will provide various other advantages, such as improving the quality of learning, improving access to education and training, reducing the costs associated with education, and improving the cost-effectiveness of education. E-learning provides a platform of a well-designed, learner-centred, engaging, interactive, affordable, efficient, easily accessible, flexible, and meaningfully distributed and facilitated e-learning environment. Moreover, students can save money and time spent on travelling and getting the right materials for their study. They can reduce printing costs by reading the available learning materials online. Furthermore, e-learning increases access to learning materials. It also enables students to have wider access to limited resources, such as e-journals and e-books. This can support the students in enhancing their learning. By eliminating barriers of time, distance and socio-economic status, individuals can now take charge of their own life-long learning.

The improved communication link and better student access encourages improved participation. Students can have public forums, allowing them to communicate with their peers, or even private

forums between the student and the lecturer or instructor. Another benefit offered by e-learning is faster delivery of assessments, as lecturers can give feedback faster compared with the traditional method, and students can also contribute to feedback amongst themselves.

2.4 Challenges in E-Learning

Implementing e-learning is not an easy task. Despite many benefit gained from e-learning, there are also issues and challenges when aiming to make e-learning successful. The challenges, as reflected in Figure 5, are considered from two perspectives: the learning provider, and the user. From the learning provider perspective, Higher Learning Institutions (HLIs) are experiencing difficulties in relation to various technological issues, such as preparing efficient infrastructure. Bandwidth and connectivity are ultimately necessary, since students will be dependent on these facilities to access learning materials on the web. Moreover, the delivery of high bandwidth content, such as digital video, is still problematic to the home user. Learning material is also an issue, since a lack of quality content is prepared. Developing good content for students should consider many different factors, such as pedagogical aspects, human-computer interface, and expertise. Ensuring all of these are well-prepared requires a high budget; thus, high costs for implementation are to be expected. In a developing country, all of these challenges are even more difficult, simply because of the resources issues faced.

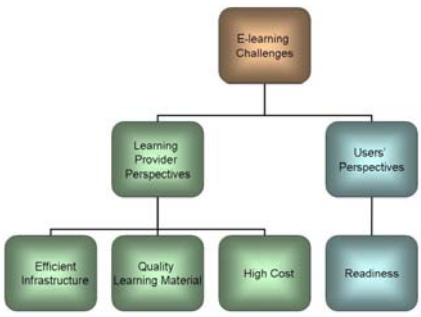

Figure 5.The E-learning Challenges

From the users' perspectives, they are experiencing challenges in the contexts of readiness. Aziz [8] proposes critical factors in preparing people readiness include commitment and skills. Readiness includes readiness of knowledge, plus readiness of motivation for self-learning. Students are not prepared for e-learning because of low computer literacy and low levels of self-discipline for self-learning methods. Furthermore, according to the Technology Acceptance Model (TAM), the perceived usefulness and perceived ease of use do have impacts on users' acceptance on the technology usage: if they don't see how e-learning can help them, the student will ultimately resist continuation, or even enrol because they think they would fail because of lack of support and training provided by the learning provider. Moreover, instructors would also feel the same; subsequently, another reason for not wanting to use e-learning is because they see little reward or recognition, yet there are so many actions to carry out so as to ensure the success of e-learning. Despite the challenges discussed above, the market of e-learning is growing. The growth of e-learning is fuelled by new institutions entering the online arena combined with a continued student demand for online learning option. Amongst the factors to be considered when developing the e-learning environment, multimedia instruction, autonomous learning, instructor-led interaction, improvement of learning effectiveness, and social presence are all considerations. These challenges are somehow related when creating secure and successful e-learning environments in the sense of confidentiality, availability and integrity. Importantly, information security in e-learning is a challenge which is rarely discussed. Security in e-learning has been disregarded and abandoned [9].

3. Information Threats in Internet

With consideration to ICT, people nowadays are getting the benefits of accessing vast information quickly. Information may exist in many forms: it can be printed or written on paper, stored electronically and transmitted by post or by electronic means. Whatever form information takes or the means by which it is shared, it should always be appropriately protected.

Information deriving from useful data is amongst an organisation's main assets. Nevertheless, when it is always easy for everybody to access, it will therefore also be easy and useful for anybody to gain access, irrespective of whether they have good or bad intention. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. As such, information must be protected in order to avoid the loss of its confidentiality, integrity and availability. Some of the most serious threats are listed as below.

1. Deliberate software attacks (viruses, worms, macros, denial of service)
2. Technical software failures and errors (bugs, coding problems, unknown loopholes)
3. Acts of human error or failure (accidents, employee mistakes)

4. Deliberate acts of espionage or trespass (unauthorised access and/or data collection)
5. Deliberate acts of sabotage or vandalism (destruction of information or system)
6. Technical hardware failures or errors (equipment failure)
7. Deliberate acts of theft (illegal confiscation of equipment or information)
8. Compromises to intellectual property (piracy, copyright, infringement)
9. Quality of Service deviations from service providers (power and WAN service issues)
10. Technological obsolescence (antiquated or out-dated technologies)
11. Deliberate acts of information extortion (blackmail for information disclosure).

3.1. Information Security in E-Learning

E-learning is mainly dependent on information as well as communication technologies. According to Rosenberg [10], e-learning is based on three fundamental criteria, which are: 1) network-capable updating, storage/retrieval, distribution and sharing of information; 2) delivery to the end of user via computer using standard Internet technology; and 3) focus on the broadest view of e-learning. The first and second criteria expose the e-learning institutions to the threats, as the use of ICT could ultimately lead to many possible information security risks which could compromise information, such as loss of confidentiality, availability, exposure of critical data, and vandalism of public information services [11]. Unfortunately, very few efforts have been made to rectify this situation. More efforts have been emphasised to enhance the content and technology due to addressing content and technology as the challenges in securing a successful e-learning environment.

Security is needed within e-learning environments owing to the fact that, nowadays, knowledge has become an important means of production, as product and as a key for personal success. In e-learning, information deriving from useful data is amongst the main assets of the organisation. Amongst security issues in e-learning are protection against manipulation (students, insider), user authentication, and confidentiality [11]. However, as the functionality of e-learning is expanding, information must be actively protected in this bigger context to avoid the loss of its confidentiality, integrity and availability. Some people might state that knowledge should be shared, but there are situations where the flow of sensitive information should be restricted to only a few well-defined groups, such as, for example, learning materials for certain groups and copyright protection of intellectual properties. Furthermore, it is difficult to verify whether or not an assignment has been completed and sent by a valid student. The identity and the secure content are difficult to maintain.

E-learning shares similar characteristics of other e-services. There are three main characteristics of every e-service: the service is accessible via the Internet, the service is consumed by a person via the Internet, and there might be a fee which the consumer pays the provider for using the e-services. The functionality and security threats to e-learning have common features with other e-services, and the management approaches could also have common characteristics. If organisations are to protect and maximise the return on their investment in learning technology, content and services, the systems they use must be interoperable, usable, manageable, and durable [12]. Previous studies have shown that there are barriers to a more wide-spread adoption of online education [6]. The reason behind such barriers is not the high costs or the greater level of tasks which need to be carried out, but rather the security aspect, which is something that is really intangible in the cyber world. Ultimately, it is difficult to verify whether or not the assignment is completed and sent by a genuine student. The identity and the secure content are difficult to maintain. Furthermore, security issues in e-learning have been addressed mostly by security technology; for example a technical framework on authentication and accountability, access control, protect of communications, non-repudiation issues and learning resource provider server protection [13].

3.2 Information Security Elements in E-Learning

Information security is the protection of information from threats. It is implemented in order to ensure business continuity and to accordingly minimise business risk. At the same time, it is expected that there be a good return on investments and business opportunities. The e-learning aims are concerned with providing teaching and e-learning to everyone. Ensuring the availability and integrity of information is the main goal in relation to e-learning security. Availability in e-learning is the assurance that the e-learning environment is accessible by authorised users, whenever needed. Two facets of availability are typically discussed, which are denial of service and loss of data processing capabilities. The e-learning users are dependent on the information on the Internet; therefore, the availability of materials and information to be accessed at any time and any location is crucial. Failing to fulfil this will have a huge impact on e-learning users and e-learning providers. Yang *et al*. [14] mention that some features which affect e-learning are privacy and security for e-delivery and collaborative education.

The availability of materials and information is inadequate. It is important to guarantee the reliability of the materials and the information published. This relates to another security element, which is integrity. Integrity in e-learning is the protection of data from intentional or accidental unauthorised changes. Integrity depends on access controls; therefore, it is necessary to positively and uniquely identify all persons who attempt access. Integrity can be compromised by hackers, masqueraders, unauthorised user activity, unprotected downloaded files, LANs, and unauthorised programs (e.g., Trojan horses and viruses), simply because each of these threats can lead to unauthorised changes to data or programs. Although availability and integrity are the main security elements which require emphasis within e-learning environments, the element of confidentiality is also important. Confidentiality is the protection of information in the system so that unauthorised persons cannot gain access. The following are some of the most commonly encountered threats to information confidentiality: hackers, masqueraders, unauthorised user activity, unprotected downloaded files, local area networks (LANs), and Trojan horses.

3.3 Research in Security of E-Learning

Securing the e-learning environment requires avoiding the four types of threat, which are fabrication, modification, interruption and interception. Currently, little research has been conducted to secure the e-learning environment. Researches in security mainly focus on three main areas: policy, identity (which refers to access management) and intellectual property.

Most researchers state that, in order to avoid all attacks upon the e-learning environment, controlling access is paramount. One of the ways to do this is via authentication and authorisation process. Jalal (2008) recommends an authentication process so as to identify a legal user process; this will overcome the illegal usage of application. A system which is too heavily secured will be difficult to be accessed by the user. In order to balance access and security, Saxena [15] mentions providing users with single sign on authentication and authorisation services to all authorised web applications and web resources. Graf [11] suggests an approach to protecting intellectual property by extending the control of the copyright holder on the entire lifetime of the digital data. He suggests a method known as CIPRESS, which controls the access to the material. Yong [16] discusses another technical aspect concerning how to secure e-learning by digital identity design and privacy preservation.

However, controlling access by using certain technology devices is considered insufficient, since the attack does not necessarily come from outsiders but could also come from the insider. The proper supervision of the handling of information security issues is important in order to ensure no vulnerabilities. Therefore, the information security management is important when striving to ensure the success of secured e-learning implementation.

4. Discussion

The success of e-learning requires facing all the challenges addressed in implementing e-learning, especially the information security challenge. Security elements, such as availability, integrity and confidentiality of material and information in place, all contribute to making the e-learning environment a secure and save environment. Moreover, students benefit from having an effective learning environment, and the e-learning provider can be comfortable with sustainable business.

4.1 Information Security Management (ISM)

Information security is the protection of information from a wide range of threats in order to ensure business continuity, to minimise business risk and to accordingly maximise return on investments and business opportunities. The goal is mainly concerned with detecting and preventing unauthorised acts of computer users. Information security is achieved by a suitable set of controls known as Information Security Management (ISM). ISM includes policies, process, procedures, organisational structures and software and hardware functions, and needs to be implemented in order to ensure that it is sensibly managing the risks. Furthermore, such controls need to be established and implemented, monitored, reviewed and improved where necessary so as to ensure that the specific security and business objectives of the organisation are met (BS ISO/IEC 17799:2005).

Many information systems have not been designed to be secure. The security which can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail [17]. A white paper written by Absolute Software stated that a survey of 185 IT professionals indicates that, whilst data breach prevention is a top priority, current data protection strategies are consistently undermined by employees. It may also require participation from shareholders, supplier, third parties, customers or other external parties. Specialist

advice from outside organisations may also be needed.

There are 10 domains listed in the handbook of ISM, which are: access controls; communication system; risk management and business continuity planning; policy, standards and organisation; computer architecture and system security; law, investigation and ethics; application program security; cryptography, operation security and physical security. All of these domains are very important, and each should be considered when ensuring the security of information.

Security management is a discipline in making trade-offs continual activity: controls in the system versus controls in the environment, security control versus customer convenience and productivity, strong controls versus implementation and administrative cost, and so on. [18]. Once a computer system has been deployed, it then needs to be managed so as to ensure that it works correctly. Whitson [19] states that the major areas of computer management include guaranteeing confidentiality, integrity, and availability of all assets.

ISM has some standards and guidelines to be followed when setting up and managing an effective ISM: for example, the British standard BS ISO/IEC 17799:2005 Information Security Management System (ISMS). The design and implementation of an organisation's ISMs are influenced by business needs and objectives, resulting security requirements, the process employed and the size and structure of the organisation.

Information security is important to both public and private sector businesses, and when striving to protect critical infrastructures. In both sectors, security will function as an enabler to achieving e-government or e-learning, for example, and also to avoid or reduce the relevant risks. Therefore, the management of information security is needed in order to maintain a competitive edge, adequate cash flow, profitability, legal compliance, and commercial image.

4.2 Information Security Management in E-Learning

At present, information security technology, hardware and software have been used in order to secure the e-learning environment. Yang *et al.* [14] suggest the obligation of having effective mechanisms for security and privacy control and management. Having a control without proper planning concerning how to manage the control does not help in reducing the threats in e-learning. An analogy to this is: to keep a house or a room of valuable data, the door is locked, using the key and lock as the control mechanism. Only the authorised people are given the key to access to the house. Unfortunately, however, the process (the management) of delivering the key to the validated people is handled insufficiently, which can consequently lead to the key ending up with malicious people. In a different situation, the key might also become lost or could be duplicated and then used by unauthorised people. Therefore, it is not only the solution or controls which matter but the management of security, which will determine the success of the security controls and solution implemented. In spite of considering the hardware and software solution, information security can be achieved by a suitable set of controls, known as Information Security Management (ISM). ISM includes policies, process, procedures, organisational structures, and software and hardware functions. Kritzinger and Von Solm [20] suggest four main elements of information security within e-learning environments, including ensuring e-learning information security governance, creating e-learning information security policy and procedures, implementing e-learning information security countermeasures, and monitoring the e-learning information security countermeasures. The elements suggested here include the management aspect to ensure that the security implementation achieve its objective.

ISM in e-learning can be stated as similar to other e-services; however, there are some different emphases based on the services being offered. E-learning offers flexibility to the user as a learner, whilst simultaneously ensuring availability, integrity and confidentiality of information. The behaviours of users in e-learning are also different from the users in other e-services; therefore, ISM is specifically needed for e-learning.

4.3 Framework

ISM is the only real opportunity for an organization to build an effective security architecture which can fight existing and emerging information security threats. Therefore, e-learning requires an ISM framework which can act as a guide in helping the e-learning provider (institutions) in terms of managing the information security within the e-learning environment. The framework should consider the e-learning context and accordingly include the appropriate and necessary elements comprised within e-services. When developing a framework, few important requirement need to be addressed. A further investigation concerned with identifying the threats and incidents of attack in e-learning needs to be conducted in order to ensure the success of ISM frameworks for e-learning.

The e-learning ISM framework should include various details on policies, process, procedures, organisational structures, and software and hardware functions so as to enhance security execution. Another aspect which should be considered is the

maintenance procedures. Security management is an important part of the whole secure system process. A system whereby security cannot be managed is not secure, no matter how excellent the controls suggested. Furthermore, the users (lecturer and students) will also benefit with the secured e-learning environment.

5. Conclusion

E-learning has grown and is expanding at a very rapid pace. The benefits it offers increase the number of e-learning users. The functionality of e-learning continues to expand and relies more and more heavily on the Internet. However, the Internet has become a place of illegal activities, which therefore expose e-learning to threats. Ensuring the availability and integrity of information and material within e-learning environments requires that countermeasures, such as security technology hardware and software, need to be implemented. Nevertheless, it is considered insufficient. Moreover, IMS is needed in order to ensure the security of the e-learning environment. ISM for e-learning is no different to other e-services; however, because of the flexibility factor offered by e-learning and different user behaviours, e-learning requires a security management framework which can act as a guide in helping the e-learning provider (institutions) in managing the information security within the e-learning environment. Furthermore, the combination of ISM and the current information security technology used will provide better results in the success of security implementation.

6. References

[1] Mason, R. and Rennie, F. (2006), *E-learning: the key concepts*, Routledge, Abingdon Great Britain.

[2] Eklund, J., Kay, M. and Lynch, H. M. (2003), E-learning: emerging issues and key trends: A discussion paper, Australian National Training Authority, Australia.

[3] Conole, G., Smith, J. and White, S. (2007), 'A critique of the impact of policy and funding', in Conole, G. and Oliver, M. (eds.) *Contemporary perspectives in E-learning Reserach themes, methods and impact on practice*, Routledge, London; New York, pp.38-54.

[4] Dietinger, T. (2003), *Aspects of E-Learning Environments* (unpublished Doctor of Technical Sciences thesis), Institute for Information Processing and Computer Supported New Media (IICM), Graz University of Technology, Austria.

[5] Morrison, D. (2003), *E-learning strategies*, Wiley Chichester.

[6] Allen, E. and Seaman, J. (2007), Online Nation Five Years of Growth in Online Learning, 1, Sloan Consortium, United States.

[7] Jain, K. K. and Ngoh, L. B. (2003), 'Motivating Factors in e-learning -a Case study of UNITAR', *Student Affairs Online*, [Online], vol. 4, no. 1, pp.21, June, 2008 available at: http://www.studentaffairs.com/ejournal/Winter_2003/e-learning.html.

[8] A. Aziz, S. H., M.Yunus, A. S., A. Bakar, K. and B.Meseran, H. (2006.), 'Design and development of learning management system at universiti Putra Malaysia: a case study of e-SPRINT. I', *WWW 06: Proceedings of the 15th international Conference on World Wide Web*, May 23 - 26, 2006, Edinburgh, Scotland, ACM, New York, pp.979-980.

[9] Raitman, R., Ngo, L. and Augar, N. (2005), 'Security in the Online E-Learning Environment', *Advanced Learning Technologies, 2005.ICALT 2005.Fifth IEEE International Conference on Advanced Learning Technologies*, pp.702-706.

[10] Rosenberg, M. J. (2001), *E-learning strategies for delivering knowledge in the digital age*, McGraw-Hill, New York.

[11] Graf, F. (2002), 'Providing security for eLearning', *Computers & Graphics*, vol. 26, no. 2, pp.355-365.

[12] Norman, S. and Da Costa, M. (2003), 'Overview of e-learning Specifications and Standards', *Open Learning Agency, and Eduspecs Technical Liaison Office*.

[13] Furnell, S. M. and Karweni, T. (2001), 'Security issues in Online Distance Learning', *VINE: The Journal of Information and Knowledge Management Systems*, vol. 31, no. 2.

[14] Yang, C., Lin, F. O. and Lin, H. (2002), 'Policy-based Privacy and Security Management for Collaborative E-education Systems', *Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002)*, pp.501–505.

[15] Saxena, R. (2004), 'Security and online content management: balancing access and security', *Breaking boundaries: integration and interoperability, 12th Biennial VALA Conference and Exhibition Victorian Association for Library Automation.*

[16] Yong, J. (2007), 'Digital Identity Design and Privacy Preservation for e-Learning', *Proceeding of the 2007 11th International Conference on Computer Supported Cooperative Work in Design,* , pp. 858-863.

[17] Trèek, D. (2003), 'An integral framework for information systems security management', *Computers & Security*, vol. 22, no. 4, pp.337-360.

[18] Abrams, M. D., Jajodia, S. and Podell, H. J. (1995), 'Information Security: An Integrated Collection of Essays', in IEEE Computer Society Press, Los Alamitos, CA, USA, pp.98-99.

[19] Whitson, G. (2003), 'Computer security: theory, process and management', *J. Comput. Small Coll*, vol. 18, no. 6, pp.57-66.

[20] Kritzinger, E. and von Solms, S. H. (2006), 'E-learning: Incorporating Information Security Governance', *Issues in Informing Science and Information Technology*, vol. 3.

