Information Security and E-learning in Virtual Environments: Current Issues and Implementation in Nigeria

I.K. Ogundoyin[1], J.O. Uhomoibhi[2], C.O. Akanbi[1] and A.A. Adigun[1]

[1]Department of ICT, Osun State University,
Osogbo, Nigeria
ibraheem.ogundoyin@uniosun.edu.ng

[2]Faculty of Computing and Engineering, Ulster University,
Northern Ireland, UK
j.uhomoibhi@ulster.ac.uk

Abstract

The wide spread and deployment of Internet facilities across the globe are encouraging participation of more users in some Internet-based applications in which e-learning is not an exemption. E-learning is a method of acquiring knowledge and skills which depends on the Internet in its execution. The Internet has become the venue for a new set of illegal activities, so e-learning environment is exposed to such threats. It is surprising that a lot of works by researchers on e-learning have been focused on development and deployment of e-learning systems without much attention given to the security of these e-learning facilities. This paper discusses the general overview of e-learning security threats. Some critical issues affecting e-learning security in the virtual environment vis-à-vis ethics, organisational management and design and implementation issues are examined and reported. Based on the review and findings on the security issues discussed, suggestions and recommendations are made on how to strengthen existing security technologies and policies. We recommended that the inclusion of our suggestions in the implementation of new organisational policies and management strategies will enhance the security of the e-learning systems. There could be considerable improvement in the technological approaches to mitigate the security challenges, if the findings and recommendations presented in this paper are incorporated into the design and implementation of security component of e-learning systems.

1.0. Introduction

Over the last two decades there has been a sharp increase in the use of e-learning systems both in education for degree delivery as well as corporate environment for training and certification purposes [1]. Information system security has been an important concern for most organizations, especially academics and business. However, very little attention has been given to information security in the context of e-learning systems. Researchers have paid so much attention to e-learning development and deployment. This is not too good for sustainability of the e-learning systems. If the issue of security in e-learning systems is not promptly attended to, the resulting effect could defeat the laudable purpose of e-learning, to make education available and accessible to all, irrespective of location and time.

E-learning has grown and is still expanding. The benefits it offers increase the number of e-learning users. The functionality of e-learning continues to expand and relies more heavily on the Internet [2]. However, the Internet has become a place of illegal activities, which exposes e-learning to threats [2]. Ensuring the confidentiality, availability and integrity of information and material within e-learning environments requires that countermeasures, in the form of hardware and software (technological measure) be implemented. Nevertheless, the technological countermeasures are insufficient [1]. Information Management Systems (IMSs) will enhance the effectiveness of e-learning systems [2]. The IMSs include policies, process, procedures, organisational structures and technology, implementation and risk assessment. Just like other e-services such as e-commerce, e-banking and e-government. e-learning systems require 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, having considered IMSs as a way to complement technological solutions which may not be adequate, security ethics is also considered as an issue which must be investigated.

No matter how effective the IMSs in place and the level of sophistication a security strategy has, if the users of such technology or e-learning systems behave unethically, there is every possibility that the security measures and policies will be challenged. To improve security strategy of e-learning systems, there is need to investigate the issue of ethics and see how its elements could be included in IMSs and security technology implementation. With this, existing security strategies and countermeasures will be strengthened and improved. Therefore, the combination of the current information security technology, management of security measures and critical investigation of security ethics will provide better results for effective security implementation in general. Particularly it will boost users' perceived security in the e-learning environment. This paper aims to explore the context of information security issues, the potential of information security management, the incorporation of elements of ethics in IMSs and in the design and implementation of security technologies.

2.0. E-learning

There are many different definitions of e-learning present in the literature, laying emphasis on different aspects. For instance, some researchers laid emphasis on the content, some on communication, and some on the technology [2]. E-learning has also been defined to cover a wide set of applications and processes, such as web-based learning, computer-based learning, virtual classrooms, and digital 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. E-learning has been defined as a component of flexible learning, which is a wide set of applications and processes, all of which use available electronic media to deliver education and training; this includes computer-based learning, web-based learning, virtual classrooms, and digital collaboration [4].

The concept of e-learning provides several advantages to educational organizations which use this technology, including short and effective training, flexibility and modularization. Most e-learning innovations have focused on course development and delivery, with little or no consideration to privacy and security as required elements [4, 5]. However, security is a growing need for high levels of confidentiality and privacy in e-learning applications, secured technologies must be put in place to meet these needs. Meeting the security requirements in an e-learning system is an extremely complex problem because it is necessary to protect the content, services, external users, internal users, and even the system administrators.

3.0. Information Security issues 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. The e-learning aims at providing education 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. The threats against availability are denial of service and loss of data processing capabilities. The e-learning users depend on the information on the Internet; therefore, the availability of materials and information to be accessed at any time and any location is crucial. Failure to fulfil this will have a huge impact on e-learning users and e-learning providers.

Some of the features which affect e-learning are privacy and security for e-delivery and collaborative education [3]. Privacy or confidentiality is the protection of information in the system so that unauthorised persons cannot gain access. Hackers, masqueraders and unauthorised user activity are some of the threats to information confidentiality. Before discussing some of the issues in e-learning security, it is important to briefly mention some of the common threats of e-learning systems.

The threats are either internal or external threats. The internal threats are caused by legitimate users of the e-learning system either accidentally or intentionally. For instance, an untrained user may divulge his or her password to a malicious user. The external threats are caused by malicious users who are otherwise known as hackers or masqueraders. The external threats aim at breaking the security of the e-learning systems intentionally so as to gain illegal access to the resources for selfish and malicious uses. There are many challenges of the e-learning system in the virtual environment with respect to threats. For instance, deliberate software attacks. This includes viruses, worms, macros and denial of service [2]. Technical software failures and errors relate to bugs, coding problems, and unknown loopholes. Another challenge is human error, i.e. unintentional user mistakes. More challenges could be attributed to deliberate acts of espionage or trespass, which is an unauthorised access to the resources in the virtual environment or illegal collection of data. A deliberate act of sabotage or vandalism is the physical destruction of virtual environment and the e-learning system. Other threats include technical hardware failures, deliberate acts of theft, compromises to intellectual property (piracy, copyright, and infringement), quality of service deviations from service providers and deliberate acts of information extortion. These are threats to an e-learning virtual environment because there can be cyber-attacks on e-learning system servers via the Internet, thereby causing the e-learning servers to be unavailable. There have been many cases of e-mail interception in which alteration is made to some e-mails.

Now, having discussed some of the threats capable of compromising the confidentiality, integrity and availability of the e-learning virtual environment, it is pertinent to also take a look at some of the critical issues affecting security breaches in the virtual environment. A critical and holistic examination of these issues will bring about clearer understanding of the threats processes. With this in place, the knowledge to strengthen existing threats countermeasures and to develop new ones will emerge and new solutions will be created. The knowledge that will be created as a result of this study will not only improve organisational policies and security management in place but will also be transformed into new enforceable policies which will be incorporated into the design and implementation of new security technologies for e-learning systems. These issues are: ethics in e-learning environment, information security management and design and implementation flaws in e-learning systems.

3.1 Ethical Issues and E-learning Security

Ethics deals with individual characters and moral rules that govern and limit our conduct [6]. Furthermore, ethics investigates questions of right and wrong, fairness and unfairness, good and bad, duties and obligation, justice and injustice, as well as responsibility and the value that should guide us [6, 7]. Ethical questions arise, when different interests of individuals conflict and thus there is need for a higher level of principles that are fair to the rights of all concerned [8]. These principles are fair in the sense that all members of the society accept them as binding, in order to solve the conflict of interests, so the principles are shared by the community, for every one's well-being [9]. A learning environment is no exception to this

mentality. There is a social contract about norms and expectations for all interactions. In regard, ethical principles mean cooperative and rational norms that have higher priority when compared with self-interests of the participants. Ethical issues are paramount to security of e-learning system in the virtual environment. If users do not behave right, there is no level or complexity of security measures in place that will not be abused. Despite the laudable and global impacts of e-learning to make education accessible to all anywhere any time, the purpose will be defeated.

The traditional problems of cheating, plagiarism, and violation of privacy, vandalism, theft, and spying into privacy has also created new issues around ethical learning practices, personal integrity and accountability despite the fact that e-learning has provided the learner with all the freedom to access and manage information. Students' motivation to engage in an unethical manner can be accounted to temptation to speed graduation , availability of convenient IT tools, a sense of entitlement and the lack of consequences, peer pressure, as well as a lack of understanding of educational purpose [11, 12, 10]. There are many ethical challenges in the form of fraud confronting e-learning systems. One of these frauds is breaching of computer ethics. Breaching computer ethics means going against code of conduct as developed by the Association of Computer Machinery (ACM), the world's largest educational and scientific computing society. It is reported [9] that the Code of Ethics lists the general moral imperatives as contributing to society and human wellbeing, avoiding harm to others, being honest and trustworthy, being fair and taking action not to discriminate, honouring the property rights such as copyrights and patents, giving proper credit for intellectual property, respecting the privacy of others and honouring confidentiality The code of conduct provides a general framework for online learning environments with its emphasis on civility of communication and using information. Any act not conforming to this code of conduct is unethical.

The nature of e-learning today has paved way for fabrication, modification, interruption and interception. All these raise questions about the position of ethics in the virtual environment. One may be tempted to ask, what has all these to do with security of e-learning systems in the virtual environment? The fact is that for any un-ethical act, there must be violation of security property of confidentiality, availability and integrity. This is a pointer to the fact that ethics has a lot to do with security. To strengthen security, and to avoid violation of rules and policies, users' ethics must be positive.

3.2 Information Security Management.

Information security is the protection of information from a wide range of threats which could jeopardise confidentiality, integrity and availability. 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) [2]. An ISM includes policies, process, procedures, organisational structures and software and hardware functions put together to manage security risks. The 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. There are many information systems today including e-learning systems, which are yet to be designed securely. The fact that technical security measures are not enough to combat the present emergent threats necessitates effective and appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail [2, 5].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. Therefore, the management of information security is needed in order to maintain a competitive edge, and legal compliance. The possession of security control without proper planning on how to manage the control does not help in reducing threats against the system in question, which may be e-learning in this context. Therefore, it is not only the security solutions or controls available at particular point in time that only matters but the management of security as well. The management goes a long way in determining the success of the security controls and solution in place. The point being stressed here is that, available controls and countermeasures must be supported with organisational policy and management. It is the management and policy in place that will dictate punishment for intentional violation of security control put in place. Therefore, e-learning information security governance, e-learning information security policy and procedures, implementation of e-learning information security countermeasures and monitoring of e-learning information security countermeasures require sound and effective management to ensure that the security objectives are achieved.

3.3. Design and Implementation Issues on E-learning Security

Another issue of e-learning system security which requires attention is the design and implementation. There are so many design issues in some e-learning systems today. This is because little attention has been paid to security in e-learning in the past. Designers and developers focussed development and deployment. Malicious users tend to look for loopholes in design and implementation of e-learning systems. The malicious users leverage the design lapses to carry out their malicious intent. Design and implementation with respect to security are such a serious issue in e-learning systems that must be taken seriously, if the desired environment void of threats and violation of privacy is to be achieved.

4.0. Discussion

The path to make e-learning achieve its laudable object of making education available and affordable for all irrespective of location and time requires creation of a safe and trusted environment. This can be achieved by proper consideration of issues raised in this paper and implementation of our recommendations as suggested in the issues raised and discussed. We have explicitly raised the issues of security ethics, security management and security implementation and design as

they affect e-learning survivability. Solving these issues will culminate into ensuring security property of availability, integrity and confidentiality of material and information handled by the e-learning systems. With this in place the e-learning will deliver its lofty objectives. Moreover, students will benefit from having an effective learning environment, and the e-learning provider can be comfortable with sustainable business.

On the issues of ethics, there should be more awareness on how to behave positively while in the virtual environment or while engaging with the e-learning systems. Users should be acquainted with best practices in conformity with international standard. All institution providing e-learning services should ensure that all students take courses in ethics, particularly computer ethics. This will go a long way in instilling positive ethics in the students who are users of the e-learning systems. Students should be made to understand the consequences of unethical behaviour in the virtual environment. Every institution offering e-learning services should make available to student handbooks containing best practices and acceptable behaviour in the cyberspace. The society must hold in esteem positive ethical and moral standard so that young ones will grow to develop positive ethics.

We have stressed that technological measures are limited in their capacity to provide the required security for the e-learning systems. It is most appropriate to complement available and new security controls with proper management and policy. Policy and management approaches have the capability to effectively manage and control large distributed systems like e-learning system. In most policy-based management systems, policies are used to change the behaviour of systems. Policies are usually expressed in terms of authorization and obligation imperatives over subject and object entities. Authorization policies define the authorized and unauthorized actions of a subject over an object; obligation policies specify the positive and negative obligations of a subject toward an object. In a policy-based e-learning system, the system administrator might specify some basic policies for the general operation of the system, and additional policies might be added based on the preferences of the entities. There should be sets of policies for each of the entities in the system (administrator, teacher, student, course material) as well as for the interaction between these entities. In addition, governments and other regulatory bodies may have privacy laws or regulations. These may be translated into electronic policies and added to the general policies.

Design and implementation of e-learning systems are critical to their security. If the design and implementation of security feature of e-learning systems is porous, malicious users will leverage it to perpetrate illicit activities on the system. Good design and implementation of security in e-learning should operate around the following:

1. Authentication and Authorisation

E-learning system should have standard users' authenticating feature. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. The permissions and folders

returned define both the environment the user sees and the way he can interact with it, including hours of access and other rights such as the amount of allocated storage space. The process of an administrator granting rights and the process of checking user account permissions for access to resources are both referred to as authorization. The privileges and preferences granted for the authorized account depend on the user's permissions, which are either stored locally or on the authentication server. This feature will go a long way in frustrating activities of unauthorised users.

2. Trust Mechanisms

Trust is an important concern in e-learning systems. In the context of networking and distributed applications, one system needs to be trusted to access another underlying system or service. Trusted interaction forms the underlying requirement between user and providers. For example, a service provider must trust that a learner truly has credentials that are not forged and is authorized to attend the course, or is limited to accessing only some services. On the other hand, the learner must trust the services. More importantly, the learner must believe the service provider will only use his/her private information, such as name, address, credit card details, preferences, and learning behaviour in a manner expressed in the policy provided for the e-learning system user. The most common trust mechanisms are related to digital certificate-based approaches and trust management systems. A Digital Certificate-based Mechanism is based on the notion that "certificates represent a trusted party". The key concept behind it is a certification authority issues to identify whether or not a public key truly belongs to the claimed owner. Trust management systems have the goal of providing standard, general-purpose mechanisms for managing trust.

3. Secure Distributed Logs

Secure distributed logs allow a record to be kept of transactions that have taken place between a service user and a service provider. The logs are distributed by virtue of the fact that they may be stored by different applications operating on different computers. Details of the transaction including the time of its occurrence would be "logged" and the resulting record is secured using cryptographic techniques, to provide assurance that their modification, deletion or insertion would be detectable. For e-learning, the use of secure distributed logs has important implications for privacy. In fact they support the Privacy Principles of Accountability, non-repudiation and Challenging Compliance. In the case of Accountability and Limiting Use, Disclosure, the existence of a secured record of transactions allows verification that conforms to each principle has been maintained. In the case of Challenging Compliance, the existence of a record is very useful for possibly showing where compliance has wavered.

4. Safeguards

This will include other security measures like data backup, cryptography, antivirus software, anti-spyware and firewalls necessary for safeguarding the e-learning system from malicious use.

5.0. Conclusion

E-learning systems enable learning through the Internet. The dependency of the e-learning systems on the Internet for their operations has exposed them to the risks ravaging the Internet. Unfortunately, attention has not been paid to the issue of e-learning systems security. In the light of this, we briefly discussed the general overview of e-learning systems and salient security challenges in the virtual environment. Issues pertinent to the security challenges of the current e-learning systems were discussed. The issues identified to have caused security loopholes include ethics, inadequate security management and poor design and implementation strategies. Recommendations were made for how existing security measures could be strengthened and the need to incorporate some of the research findings not only into organisational management policies but also in the design and implementation of the new security technology. We have recommended that the development of the e-learning systems should be done using internationally recognized methods and safety standards. The e-learning systems need to implement security services such as authentication, encryption, access control, managing users and their permissions. Good ISM practice should be encouraged to complement technological security solution and positive ethics should be encouraged among users of e-learning system in the virtual environment.

6.0 References

1. Yair L. and Michelle M. R.., Students' Perceived Ethical Severity of e-Learning Security Attacks. *Proceedings of the Chais conference on instructional technologies research 2010: Learning in the technological era.* The Open University of Israel 2010.
2. Najwa Hayaati Mohd Alwi and Ip-Shing Fan (2010). E-Learning and Information Security Management. *International Journal of Digital Society (IJDS),* Volume 1, Issue 2, pg148 – 156
3. Yang, C., Lin, F. O. and Lin, H., '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, 2002.
4. Ciobanu C. and Ciobanu N.(2012). E-learning Security Vulnerabilities. *Procedia - Social and Behavioral Sciences.* 46 (2012) 2297 – 2301
5. Iacob, N., The use of distributed databases in e-learning systems, *Proceeding of the World Conference on Educational Sciences*, pp 2673 2677, Instanbul, Turkey 2011.
6. Show, W. H., *Business ethics (6th ed.), Belmont Thompson-Wadsworth* 2008
7. Molnar, K. K. Kletke, M. G., and Chongwatpol, J. (2008). Ethics vs. IT ethics: Do undergraduate students perceive a difference? *Journal of Business Ethics*, 83, 657-671.

8. Khalil E., Larry K., Yuefei X., and George Y. (2003). Privacy and Security in E-Learning, *International Journal of Distance Education*. 1 (4), 1-15.

9. Toprak E., Özkanal B., Aydin S. and Kaya S. (2010). Ethics in E-learnig *The Turkish Online Journal of Educational Technology*. 9 (2),78- 86

10. Brown, E. (2008). Ethics in e-Learning *Revista de Educacao do Cogeime*. Pg 211 – 216

11. Molnar, K. K. Kletke, M. G., & Chongwatpol, J. (2008). Ethics vs. IT ethics: Do undergraduate students perceive a difference? *Journal of Business Ethics, 83*, 657-671.

12. Nguyen, N. T. and Biderman, M. D. (2008). Studying ethical judgments and behavioral intentions using structural equations: Evidence from the multidimensional ethics scale. *Journal of Business Ethics, 83*(627–640).

13. ACM Code of Ethics, accessed 20/3/2015 http://www.acm.org/about/code-of-ethics.