CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION

I.Bandara, F.Ioras, K. Maher

Buckinghamshire New University (UNITED KINGDOM)

Abstract

Cyberspace refers to the boundless space known as the Internet. Cyber security is the body of rules put in place for the protection of this cyberspace. The increasing use of e-Learning systems has been documented by numerous studies and shows continuing growth; little attention has been given to the issue of security of e-Learning systems both in research and education.

In this paper, we illustrate an approach to understanding, evaluating, monitoring, measuring and managing cyber security as it relates to e-Learning systems. Security of e-Learning systems represents a unique challenge as numerous systems are accessed and managed via the Internet by thousands of users over hundreds of networks. Moreover, this paper reveals the prevalence of internal cyber-attack as well as a lack of proper IT policies and procedures in e-Learning systems, in light of their standard architecture and their specific security requirements.

Also, we discuss the most important security challenges that can be relevant for distributed e-Learning systems. Because e-Learning systems are open, distributed and interconnected, then security becomes an important challenge in order to ensure that interested, and authorised, actors only have access to the right information at the appropriate time.

Keywords: Cyber security, e-Learning systems, cyber-attack, IT policies, distributed e-Learning.

1 INTRODUCTION

E-Learning is widely used as a method of learning that ultimately depends on the Internet in its execution. E-Learning systems epitomise computing systems and networks of the Internet generation. These systems are complex and they aim to guarantee the satisfaction of the learner and maintain the good image of the learning process. There is clear evidence that innovative educational technologies, such as e-Learning, provide unprecedented opportunities for students, trainees and educators to acquire, develop and maintain core skills and essential knowledge [1]. However, e-Learning systems employ the Internet as a place to obtain all necessary information and knowledge. Unfortunately, the Internet has also become the venue for a new-fangled set of illegal activities, so-called cyber-crime. Information associated with the e-Learning environment, some of which might be personal, protected or confidential in nature, is then continuously exposed to security threats because e-Learning systems are open, distributed and interconnected.

E-Learning has gone through a spectacular development during the past years [2]. E-Learning systems are diverse and widespread, with examples including WebCT, Moodle and Blackboard. They are large and dynamic with a variety of users and resources. The sharing of information, collaboration and interconnectivity are core elements of any e-Learning system. Data must then be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user authentication and compromises in confidentiality are important security issues in e-Learning. Meanwhile, e-Learning trends are demanding a greater level of interoperability for applications, learning environments and heterogeneous systems.

The purpose of this paper is to provide an overview of the most important cyber security challenges that are relevant to Higher Education systems and future distributed e-Learning systems. The main sections will cover: cyber security and education; security threats, detection and protection in distributed e-Learning systems; developing a security management model for e-Learning systems; and, finally, some conclusions are presented.

2 CYBER SECURITY AND EDUCATION

The Higher Education sector is increasingly exploring the use of information systems and technology to meet the needs and expectations of diverse learners who demand more than just traditional classroom-based experiences. New course delivery models attempt to blend face-to-face elements with e-Learning, Webinars and other online digital content. Building trust and encouraging engagement amongst users of online learning systems is important because there are opportunities for both synchronous and asynchronous interactions with the system. Synchronous learning occurs in real-time, with all participants interacting at the same time, while asynchronous learning is self-paced and allows participants to engage in the exchange of ideas or information without the dependency of other participants′ involvement at the same time [5].

2.1 Building digital trust

Higher Education is a very different environment to what it was several years ago and is now offering significant student engagement via online learning systems. Students have an increasing understanding of information systems (IS) and information technology (IT) issues, so overall learning strategies devised by course providers must be intrinsically linked with IS/IT strategies to meet student needs now and in the future. Digital natives and digital immigrants will share high expectations of their e-Learning system, in terms of usability, security and protection of their personal information. This could include the secure handling of a student's bank details associated with payments for course fees and other products.

Universities in the UK hold significant intellectual property through research and other academic materials, which could be attractive targets for cyber-criminals. Researchers will expect their sensitive work and commercially important information to be securely stored, with no risk of theft or misuse.

Institutions should perform a cyber security risk assessment and determine best arrangements for technology, people and processes.

2.2 Bring your own device and remote access

Bring your own device (BYOD) raises a number of data protection concerns due to the fact that the device is owned by the user rather than the data controller. Students are comfortable using technology for communication, finding information, for collaboration and as a platform for their learning and development. They also want wireless and on-demand access to the university network, including any virtual learning environment, not only through the university's own fixed PCs in dedicated computer rooms but also via their own device (tablet, smartphone) from different locations on and off campus.

It is crucial that the data controller ensures that all processing of personal data under his control remains in compliance with the Data Protection Act (DPA) 1998. The DPA is based around eight principles of 'good information handling' [3]. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it. The specific risks that a BYOD policy addresses will be unique to each organisation. An important question to consider is: Which personal data can be processed on a personal device and which must be held in a more restrictive environment? Universities and organisations must consider if those students, academics or employees using their own devices are processing non-corporate information about the owner or other users of the device. Nevertheless, it remains crucial that users are managing any pertinent personal information in compliance with DPA principles.

2.3 Security in learning management systems

Current e-Learning systems supporting online collaborative learning do not sufficiently meet essential security requirements [4]. Collaborative learning experiences are normally designed and implemented with pedagogical principles very much in mind, whilst security issues are largely ignored. This may lead to undesirable situations that have a detrimental impact on the learning process and its management, such as students falsifying course assessments, presenting a convincing false identity to others, intrusion upon controlled or private conversations, alteration of date stamps on submitted work, and a tutor gaining access to the personal data of students.

Moneo *et al.* [4] propose the use of an approach based upon Public Key Infrastructure (PKI) models that offer essential security properties and services in online collaborative learning, such as availability, integrity, identification and authentication, access control, confidentiality, non-repudiation, time stamping, audit service and failure control.

PKI assumes the use of Public Key Cryptography; it is the most shared method on the Internet for validating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, Public Key Cryptography and Public Key Infrastructure is the preferred approach on the Internet.

2.4 Highest cyber security threats in higher education

Mobile devices are being utilised by the enthusiastic and early adopters of technology, with new devices pervading campuses across the country. Many new and advanced mobile devices (such as, iPads, new Android phones, tablet devices and portable Internet access systems) are launched daily with upgraded versions of operating systems; these are ripe for infection and ready to infect a university's network system. It is then important to support these devices, whilst maintaining complete visibility of their connectivity and interactions with the university system.

2.4.1 Viruses and Social Media

University and college students are the biggest users of social media, for example, Facebook, Twitter, and YouTube. This will enable the hosting and spreading of Malware, and other viruses like Wildfire, through social media sites. It will be virtually impossible to permanently block access to social media on a college or university campus. Quick identification of infected devices is essential in order to maintain network security and protect crucial data.

2.4.2 Virtualisation of desktops to servers

Virtualisation is a widely used and popular strategy in all types of enterprises including those in Higher Education. The system offers significant savings on hardware and management costs, supports the implementation of a green strategy, as well as taking advantage of the move to virtualised desktops. When more users move to virtualised environments, more threats will arise. Higher Education institutions need to remember that hosted virtualised desktops (HVDs) should be viewed in the same way as traditional devices, posing the same threats as any connected device.

2.4.3 Consumerisation of IT

IT consumerisation is driven by users who buy their own devices, use their own personal online service accounts, install their own applications and then connect to the university or corporate network with the device - often without the organisation's knowledge or approval. In the Higher Education sector, an institution's own consumerisation of IT has made the problem even more difficult to manage. As users increasingly adopt their own devices for professional use, Higher Education institutions will see more network security threats. In fact, the consumerisation of IT is driving the need for network security solutions that can cover multiple types of devices and infrastructure components. It is necessary to respond with security solutions that identify any consumer-adopted device, scan for threats and deficiencies and then provision access or automatically remediate problems, regardless of the type of device or location.

3 SECURITY THREATS, DETECTION AND PROTECTION IN DISTRIBUTED E-LEARNING SYSTEMS

E-Learning systems share the same characteristics and challenges as other e-services, requiring the sharing and distribution of information. More specifically, they are associated with the accessibility of service via the Internet, the consumption of services by a person via the Internet and the payment for a service by a customer. Organisations must put greater emphasis on security risk management, taking into consideration the type and severity of the different threats and vulnerabilities, and recognising the diverse interaction and integration between clients, servers, databases and other components.

3.1 Cyber security issues for distributed e-Learning systems

E-systems are vulnerable to a number of threats: serious security threats include software attacks (viruses, worms, macros, denial of service), espionage, acts of theft (illegal equipment or information) and intellectual property (piracy, copyright, infringement). E-Learning systems do have some peculiarities, having a variety of users, multiple applications and information to download and upload [7].

E-systems are vulnerable to a range of security threats (summarised by Rjaibi *et al.*[8]):

- **Authentication** – broken authentication and session management; insecure communication.
- **Availability** – denial of service.
- **Confidentiality attacks** – insecure cryptographic storage; insecure direct object reference; information leakage and improper error handling.
- **Integrity attacks** – buffer overflow; cross site request forgery; cross site scripting; failure to restrict URL access; injection flaws; malicious file execution.

A threat is defined as a category of object, person or other entities that presents a danger, such as Trojan horses or phishing. Schemes that involve password-based authentication of users are highly susceptible to phishing attacks, which are becoming more and more sophisticated and require strong preventative and countermeasures [12].

Rjaibi *et al.* [8] have also proposed and illustrated the use of a Mean Failure Cost (MFC) model for managing and quantifying security threats, paying appropriate attention to: the basic architectural components of an e-Learning system; the different stakeholders; the various security requirements; the different types of security threats.

3.2 Privacy concerns in e-Learning

May and George [12] have acknowledged the technical and ethical aspects of using a tracking system to observe and analyse the different human-computer interactions that occur as part of computer-mediated learning (CML) in e-Learning, distance learning and blended learning. They have raised awareness of security and privacy protection as important issues for practitioners and researchers where student tracking and personal student data are utilised. An improved understanding of the security issues will help participants to avoid security threats as well as improving their own protection and that of their learning environments [9].

The providers of the virtual learning environment, and the tutors distributing the content, are concerned with delivering a secure learning environment and the safe storage of confidential learner data. The learners themselves make a trust judgement about the learning environment, and are interested in the protection of their sensitive personal data [10]. Data collected about the issues of privacy and security in technology-enhanced learning [11] established that people perceived different aspects in the following order of decreasing importance: awareness raising > protection of personal data > authenticity of learning resources > seamless access > address and location privacy > single sign-on > digital rights management > legislation > anonymous use.

3.3 Information security management in e-Learning

Alwi and Fan [14] have reviewed the security issues that relate to e-Learning systems. They have presented a useful overview of the most serious threats:

- **Deliberate software attacks** (viruses, worms, macros, denial of service);
- **Technical software failures and errors** (bugs, coding problems, unknown loopholes);
- **Acts of human error or failure** (accidents, employee mistakes);
- **Deliberate acts of espionage or trespass** (unauthorised access and/or data collection);
- **Deliberate acts of sabotage or vandalism** (destruction of information or system);
- **Technical hardware failures or errors** (equipment failure);
- **Deliberate acts of theft** (illegal confiscation of equipment or information);
- **Compromises to intellectual property** (piracy, copyright, infringement);
- **Quality of Service deviations from service providers** (power and WAN service issues);
- **Technological obsolescence** (antiquated or out-dated technologies);
- **Deliberate acts of information extortion** (blackmail for information disclosure).

Table 1, describes protection against data manipulation, user authentication and confidentiality as important security issues in e-learning.

Chen and He [15] reviewed the academic research literature in order to discover the main security risks and protection measures in e-Learning systems (online learning).

Table 1: Protection against data manipulation, user authentication and confidentiality

Security risks	Protection measures
• ARP cache poisoning and MITM attack • Brute force attack • Cross-Site Request Forgery (CSRF) • Cross Site Scripting (XSS) • Denial of Service (DoS) • IP spoofing • Masquerade • Rootkits • SQL Injection • Session Hijacking • Session Prediction • Stack-smashing attacks	• Installing firewalls and anti-virus software • Implementing Security Management (ISM) • Improving authentication, authorisation, confidentiality, and accountability • Using digital right management and cryptography • Training security professionals

Information Security Management (ISM), including policies, processes, procedures, organisational structures, and, software and hardware functions, needs to be properly implemented in order to properly manage and mitigate against risks and threats.

4 IMPLEMENTING A SECURITY MANAGEMENT MODEL FOR E-LEARNING SYSTEMS

Higher Education institutions should implement corporate approaches to managing their information security risks as part of existing governance structures. Institutions have to identify the 'controls' of data in order to establish clear lines of secure information sharing in a distributed environment. Implementing cyber security governance needs appropriate levels of understanding of the threats facing the university and the measures that must be put in place. It will require the allocation of day-to-day responsibilities for assessing, managing and reporting risks appropriately [6]. Principles, heads of schools/departments, all the academic staff and the IT support group in the Higher Education establishment should be clear about their own responsibilities and stay alert to the emerging and evolving threats and risks to data users. In Figure 1, the process model developed for managing cyber security threats in Higher Education systems is illustrated.

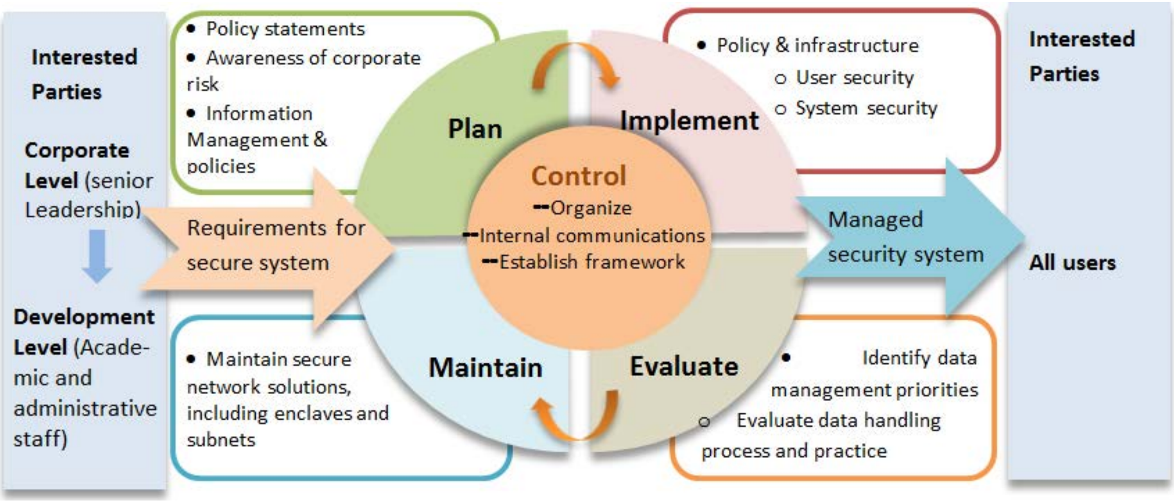
Interested Parties
Corporate Level (senior Leadership)
Development Level (Academic and administrative staff)
• Policy statements
• Awareness of corporate risk
• Information Management & policies
Requirements for secure system
Plan
Implement
Control
--Organize
--Internal communications
--Establish framework
Maintain
Evaluate
• Maintain secure network solutions, including enclaves and subnets
• Policy & infrastructure
o User security
o System security
Managed security system
• Identify data management priorities
o Evaluate data handling process and practice
Interested Parties
All users

Figure 1: Managing cyber security threats in Higher Education institutions: process model for security system

The diagram shows how various stakeholders (staff and users) contribute to and are impacted by a well-managed approach to cyber security in the organisation. Identification and specification of requirements represents the input (from the left-hand side) to a process cycle with Plan, Implement, Evaluate and Maintain stages. This Control cycle is continuing, repeating and goes through appropriate amendments and iterations, in response to the information and intelligence available, such that the output (on the right-hand side) is a managed security system. Effective stakeholder adoption, with clear direction and expectations communicated from management about user responsibilities and behaviour, is crucial for the success of such a security model.

All the Higher Education institutions should be aware of their duties regarding the protection of institutional and research data and have appropriate measures in place to ensure that they are compliant with the Data Protection Act (1998) [6]. Most of the Higher Education institutions will have different structures for the management of data and research, and appropriate levels of oversight. There will be a variety of data management policies and plans in operation, with very little consideration given to errors. These features present a challenge for corporate governance to both respect the issues and understand the real need for a process model to manage, control and mitigate against employee cyber security threats.

Eventually, network security is a responsibility for the whole institution. Network administrators and protectors can maintain up-to-date knowledge of threats and counter measures through exchange of information with peers, government and others. The contribution of users cannot be underestimated in the security of any network and related information. They must play a central role in evaluating the risks posed to information, appreciating security priorities, and, finally, taking responsibility for the implementation of controls [6].

5 CONCLUSIONS

The demand for e-Learning has changed the way in which Higher Education conducts its core business of providing courses to various learners. Organisations must find and implement new services that can enable students to study effectively and securely in a virtual environment. The increased demand from e-Learners for flexibility, mobility and empowerment poses a significant challenge to Higher Education IT departments, who are finding it harder to maintain control over how data is used, stored and shared inside and outside the virtual class. The implementation of new services, to meet demanding user needs, requires the building of secure, standardised, highly available e-Learning environments, as well as centralised application management.

ACKNOWLEDGEMENT

This article was supported by work conducted under the Tempus European project entitled 'Enhancement of cyber educational system of Montenegro' (544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES).

REFERENCES

[1] Scott P. and Vanoirbeek C. (2007). Technology-Enhanced Learning. Technology-Enhanced Learning, vol. 71, pp. 12-13.

[2] Rabai L. B. A. and Rjaibi N. (2012). Quatifying Security Threats for E-learning Systems. Education and e-Learning Innovations (ICEELI), 2012 International Conference, Tunis, Tunisia, July,2012.

[3] ANON, (1998). Data Protection Act 1998; Bring your own device (BYOD) ICO, 1998. [Online]. Available: http://ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.ashx [Accessed 20 09 2014].

[4] Moneo J. M., Caballe S. and Prieot J. (2012). Security in Learning Management Systems. eLearning Papers, Catalonia, Spain.

[5] Johnson H. (2007). Dialogue and the Construction of Knowledge in E-Learning: Exploring Students' Perceptions of Their Learning While Using Blackboard's Asynchronous Discussion Board. European journal of open, distance and e-learning, no. ISSN 1027-5207.

[6] ANON, (2013). Cyber security and universities: managing the risk Universities UK, November 2013. [Online]. Available: http://www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf [Accessed 25 09 2014].

[7] Nickolova M. and Nickolov E. (2007). Threat model for user security in e-leaning systems. International Journal "Information Technologies and Knowledge", vol. Vol.1 / 2007 , p. 341.

[8] Rjaibi N., Rabai L. B. A., Aissa A. B. and Louadi M. (2012). Cyber Security Measurement in Depth forE-learning Systems. International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2(11), pp. 1-15.

[9] Weippl E. R. (2005). Security in e-learning eLearn Magazine, 2005. [Online]. Available: http://elearnmag.acm.org/featured.cfm?aid=1070943 [Accessed 25 09 2014].

[10] Anwar M. and Greer J. (2011). Role- and Relationship-based Identity Management for Privacy-enhanced E-learning. The University of Saskatchewan, Department of Computer Science.

[11] Wolpers M. and Grohmann G. (2005). Technology Enhanced Learninig and Knowledge Distribution for the Corporate World. Int J.Knowl, Learn, 2005.

[12] Sood S. K. (2012). Phishing Attacks: A Challenge Ahead. elearning papers, April 2012. [Online]. Available: http://www.openeducationeuropa.eu/en/paper/cyber-security-and-education [Accessed 25 09 2014].

[13] May M. and George S. (2011). Privacy concerns in e-Learning: Is using a tracking system a threat? International Journal of Information and Education Technology 2011, Volume 1, Number 1. [Online]. Available: http://liris.cnrs.fr/Documents/Liris-5266.pdf [Accessed 25 09 2014].

[14] Alw N. and Fan I.-S. (2010). E-Learning and Information Security Management. International Journal of Digital Society, vol. Volume 1, no. Issue 2.

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

[16] Chen Y. and He W. (2013). Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning, 2013. [Online]. Available: http://www.irrodl.org/index.php/irrodl/article/view/1632/2712 [Accessed 15 09 2014].