Chapter 14

Learning Management Systems: Understand and Secure Your Educational Technology

Sharon L. Burton
American Meridian University, USA

Darrell N. Burrell
Florida Institute of Technology, USA

Dustin Bessette
National Graduate School of Quality Management, USA

Rondalynne McClintock
Claremont Graduate University, USA

Kim L. Brown-Jackson
National Graduate School of Quality Management, USA

Shanel Lu
National Graduate School of Quality Management, USA

ABSTRACT

Learning management systems (LMSs) are significant in offering highly collaborative, widely accessible, and manageable learning solutions. It is feasible that learning solutions stakeholders pursue an in-depth understanding of the LMS and the vulnerabilities surrounding technology-enabled learning and teaching. The over 300 types of active LMSs, proprietary or open source, are not off limits to hackers. Past research shows that hackers compromise technology systems to ascertain personal identifiable information and interfere with the integrities of post-secondary institutions. Stakeholders must understand how to safeguard the LMS. To address LMS cybercrime concerns, this text reviews vulnerability information on over 12 LMS features. After reading this text, stakeholders will gain increased insight into their works to thwart security related LMS incidents. This text can support stakeholders’ knowledge in actions to take prior to the LMS reaching unacceptable vulnerability levels. Researchers and practitioners will benefit from this text’s perspective on the LMS and mitigating risk.

INTRODUCTION

Education and learning are not about immediate learner results. Education and learning are components that shape a lifetime, and form a pathway for possibilities into the future. The upsurge of computers, information and communication technologies, and swift development of the Internet drive colleges and universities to alter their educational programs. Technology persists to have a key impact on institutions.

DOI: 10.4018/978-1-4666-8345-7.ch014
of higher learning (Glenn, 2008). The embracing of technology mediated learning, in particularly LMSs, and web-based applications resulted in a major transformation in the way researchers work together on a universal scale (Glenn, 2008).

A conduit for channeling education is the LMS, an integrated computer system that can be web-based. Learning management systems are essential tools in the higher education arena and in many businesses. According to Vogten and Koper (2014), LMSs have sufficient authenticity in an information-based society that is continually embracing cloud technology. Through the swift development of information technologies, learning management systems are one of the most significant modernisms for delivering education. The primary purpose of this ubiquitous learning management system is to provide strategic virtual educational environments and opportune communication channels between instructors and students. This virtual dimension in education supports educational institutions and learners in conquering barriers such as time and space.

Despite the affects, LMSs are popular to study because the systems continuously evolve. If this unremitting change remains inappropriately managed, the change can lead to data compromise. This text explains the LMS, the value of the LMS to a technology strategy, and browser neutrality. Further, the text provides information on the general components of the LMS, and LMS quality such as the software as a service phenomenon, as well as operational sustainability. As posited by Al-Busaidi, 2009; Cheng, 2011; Wang & Chiu, 2011, LMS quality is related to the attributes of the system (i.e., functionality, interactivity). For the purpose of this text, functionality is the specific use or set of usages in that the LMS was designed and developed.

This LMS examination supports thought leaders - Chief Learning Officers, Chief Information Officers, and other Learning and IT professionals in efforts to understand better the LMS, and comprehend vulnerabilities of such systems, combat information leakage, and guard against data contamination. This text provides these thought leaders, as well as stakeholders, with information to guide policymaking, and comprehend how to analyze data for adopting new systems and mitigating risks. After reading this text, practitioners and academicians will be able to enhance their understanding of LMS vulnerabilities from an operational standpoint, not as IT professionals.

WHAT IS THE LEARNING MANAGEMENT SYSTEM ABOUT?

The LMS, a system that has gained a solid position in colleges and universities internationally (Glenn, 2008), and is known by multiple names (Goyal & Purohit, 2010). Names include but are not limited to course management system - CMS (Lane, 2009; Unal & Unal, 2011), learning management system - LMS (Caminero, Hernandez, Ros, Tobarra, Robles-Gomez, Pastor, 2013; Hustad & Arntzen, 2013), and content management system - CMS (Black, 2011). Additional names given by Monarch Media Inc. (2010) are virtual learning environments (VLE), and collaborative learning environments.

The LMS can be a web-based distance education system (Deperlioglu, Sarpkaya, & Ergun, 2011), as well. Organizations are continuously looking towards technology as a way to better manage infrastructure and improve delivery of IT services and applications. Whether as a proprietary or an open source system, LMSs can affect the core business of teaching, learning, and managing learning delivery.

In 2008, Glenn reported the results of a survey providing that “60%” (p. 5) of the survey respondents said “technological change occurring in our midst will alter the perception of the college campus from a one-dimensional (physical) concept to a multi-dimensional (physical and online) one” (p. 5). Not only