Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University

Michelle Ramim, Nova Southeastern University, USA
Yair Levy, Nova Southeastern University, USA

EXECUTIVE SUMMARY

The growing use of e-learning systems has been documented by numerous studies (Levy, 2005). Yet in spite of this enormous growth, little attention has been given to the issue of security of e-learning systems both in research and in practice. Security of e-learning systems has a unique challenge as these systems are accessed and managed via the Internet by thousands of users over hundreds of networks. However, the Internet can pose security threats such as unauthorized access, hacking/cracking, obtaining sensitive information, and altering data and configuration, as well as enabling academic misconduct incidents (Freeh, 2000; Ramim, 2005; Sridhar & Bhasker, 2003). At the same time, cyber attacks have proliferated significantly in recent years. As a result, proper IT policies and procedures, in particular ones related to security of information systems, have become critical for organizations. This case study was written from the IS consultant’s point of view and addresses the issues related to insider cyber attacks combined with novice IT management knowledge in a small university. After a year of substantial growth to its online learning program, the university in this case study experienced a devastating event that halted all academic activities enabled by the institution’s e-learning system. This case reveals that internal cyber attack as well as lack of proper IT policies and procedures all resulted in multiple instances of damage to the e-learning system. The case provides detailed documentation on the security audit performed as well as stimulation for class discussions on actions to be taken as a result of the insider’s cyber attack. Additionally, this case study attempts to provide a starting point on discussions in the area of security related to e-learning systems. It is hoped that this case study will stimulate discussions among practitioners and researchers related to e-learning systems security, and that it will help prevent such incidents from occurring at other academic institutions.

Keywords: cyber crime; e-learning systems; e-learning systems security; insider cyber attack; insider cyber threats; insider IS misuse; IT policies; IT procedures

ORGANIZATIONAL BACKGROUND

Knowledgeville University (KU) is a small higher education institution with mostly minority students in the Southeastern US. KU provides undergraduate and master’s degrees in nine academic programs. The student body is about 1,200 students with most students attending full-time courses. However, a substantial number of students (20%) are enrolled on a part-time
basis in the online learning program, which is enabled by KU’s e-learning system. KU began to use its e-learning system during the 2001-2002 academic year. KU’s IT department has been managing the technical administration of this program while a faculty member was appointed to recruit, coach, and encourage other faculty members to integrate their curricula into the e-learning system. A year later, during the 2002-2003 academic year, KU had 84 courses using the e-learning system. KU had about 120 faculty members of which, at that time, 42 were using the e-learning system on a daily basis.

KU’s e-learning system is a proprietary, fully developed comprehensive online course management system (WebCT). Since 2001, online courses have been an important part of KU’s vision by enabling students’ learning in a flexible “any time, any place” mode. Consequently, online courses have been explored by KU’s administration as a new opportunity for reaching distant and local working students, as well as a new revenue stream. The online courses have become a competitive edge for KU among other small academic institutions in the region. KU’s president, Dr. Lopez, has committed to the success of the online learning program by incorporating the participation of faculty members in teaching online courses as part of their tenure and promotion review criteria. Additionally, Dr. Lopez has provided department chairs with incentives to help stimulate even further the use of the e-learning system both for on-campus courses and for fully online courses. Moreover, Dr. Lopez has allocated a moderate budget for the purchase of laptops for faculty members and for selected bright students who participate in online learning courses. Dr. Lopez also developed a set of strategies by which students, faculty, and administrators will incorporate the use of technology and the Internet in most of the daily activities on campus, quite apart from the online learning program. In every on-campus classroom building, KU now houses several multimedia classrooms and computer labs. The library purchased access to multiple electronic databases as well as acquiring several kiosk stations with Internet connection for students’ use. Each full-time faculty member was provided with a computer system and basic software package. Residential halls were equipped with several kiosk stations in the lobby and a small computer lab in each hall. The president’s office conducted annual surveys to assess students’ and faculty members’ technology skills. Consequently, as of the Fall 2002 term, all students were required to enroll in a technology course during their freshman year. Faculty who demonstrated low technology skills were encouraged to participate in technology training sessions provided by the Human Resources (HR) department. The use of the institution’s e-mail system was regularly promoted during registration events. Although registration was not Web-enabled, Dr. Lopez hoped that Internet registration would be in place by 2005.

SETTING THE STAGE

KU’s IT department was comprised of an IT director, Mrs. Rodriguez; a network administrator; two technicians who supported the entire institution; an IS consultant, Ms. Maya; a Webmaster; and a telecommunication subcontractor. Aside from Ms. Maya, all employees had been with the department for several years (4-10) and enjoyed interacting with the rest of KU’s employees on a first-name basis. Mrs. Rodriguez reported directly to Dr. Lopez, KU’s president. With 10 years’ employment with KU, she was the most senior in the department. However, she had very minimal IT knowledge and had been promoted to the position of the IT director primarily due to her seniority. Mrs. Rodriguez’s specific knowledge was in the area of accounting and finance, where she was very instrumental in helping implement the HR and student management systems. Mr. Perez had been KU’s network administrator; over the course of several months he came late to work, took extensive lunch breaks, and had overall low performance. As a result, Mr. Perez was asked to leave, and Mrs. Rodriguez assumed his responsibilities until a new network administrator could be hired. See Figure 1 for KU’s IT department organizational chart.
Related Content

An Integrative Approach to User Interface Design
www.irma-international.org/chapter/integrative-approach-user-interface-design/13392/

Critical Realism as an Underlying Philosophy for IS Research
www.irma-international.org/chapter/critical-realism-underlying-philosophy-research/13669/

Emergency: A New Ambulance Despatch System
www.irma-international.org/article/emergency-new-ambulance-despatch-system/44591/

Information and Communication Technology Management
www.irma-international.org/chapter/information-communication-technology-management/28132/

Graph Encoding and Transitive Closure Representation
www.irma-international.org/chapter/graph-encoding-transitive-closure-representation/13805/