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

Article in Journal of Cases on Information Technology · October 2006

2 authors, including:

Yair Levy
Nova Southeastern University

Some of the authors of this publication are also working on these related projects:

Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals’ Cybersecurity Skills View project

Social Engineering Exposure View project
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.
KU’s IT department has four primary functions:

1. To provide technical support and orientation to students
2. To support and maintain the computer laboratories throughout campus as well as in the library
3. To provide technical support and various IT training to faculty members as well as to maintain faculty members’ computers, software, and Web sites
4. To support and maintain the university’s administration computing and the IT equipment of all KU’s systems/functions (i.e., registration, tuition payments, financial aid, bookstore’s point of sale, cafeteria’s point of sale, grade reporting system, e-learning system, KU’s Web site, financial reporting, human resources, and IT training)

Most of the equipment in KU’s IT department had been donated from various equipment providers (i.e., Dell, HP, Cisco, etc.) where it was outdated and inadequate to perform most of the IT tasks required. KU’s IT network infrastructure consisted of the following hardware:

- An HP mainframe where the institution’s administrative datacenter and main computing were hosted (student registration, financial aid, student housing, etc.)
- An e-mail server
- A server that hosted faculty members’ Web pages as well as KU’s Web site, and additional faculty members’ server-end software used for teaching purposes
- A server that hosted the e-learning system application (WebCT)
- A server that hosted human resources application and data (payroll system)
- A server that hosted the library application and databases
- A server that hosted the bookstore point of sale application and data
- A server that hosted the cafeteria’s point of sale application and data
- A server that hosted student access and a special debit card system
- A server that hosted server-end music software (used mainly by the music department)
- Two network-enabled HP printers that provided executive reports
- A dedicated T1 line connecting KU to the Internet
- Multiple Cisco switches and 16 port hubs
KU’s IT department had no security policies and procedures as most of the activities in the department lacked formality. There was no evidence of a physical security mechanism in the server farm. Additionally, there were no mechanisms for network security in place. Moreover, technology manuals, warranties, and certificates were dispersed in various areas in the IT office.

CASE DESCRIPTION

In late 2002, KU experienced a cyber attack to its e-learning system that resulted in the server that hosted the e-learning system application shutting down in the middle of the semester, putting a halt to students’ and faculty members’ academic work. In order to assist in understanding the issues addressed in this case, the following section will provide an overview of insider cyber attacks, followed by a description of the approach to the problem proposed by Ms. Maya in the days following the cyber attack. Moreover, a review of the e-learning security audit process conducted, as well as the audit results and action plans, are discussed.

Insider Cyber Threats and Attacks

The knowledge-based economy has been mainly powered by technology-enabled communication and systems (Zang, Zhao, Zhou & Nunamaker, 2004). Additionally, enterprisewide systems and global communication have increasingly become an integral part of today’s organizations (Hamin, 2000). Corporations have increased their dependency on enterprisewide systems and global communication networks (Garfinkel, Gopal & Goes, 2002; Magklaras & Furnell, 2002). E-learning systems have been getting increased attention and have become center-stage systems in many organizations (Levy, 2006). Hamin (2002) noted that the dependency on information systems has caused organizations to “become more exposed and vulnerable to an expanding array of computer security risks or harms and inevitably to various kinds of computer misuse” (p. 105). At the same time, newer technologies along with industry regulations (i.e., Sarbanes-Oxley Act) promote substantial investment in IT security products and such investment is predicted to reach $13.5 billion by 2006 (Hale & Brusil, 2004; Schultz, 2003). However, it has been observed that most small to mid-size business organizations do not employ a security management program (Keller, Powell, Horstmann, Predmore, & Crawford, 2005). Moreover, the latest report of the Computer Security Institute (CSI/FBI) (Gordon, Martin, William, & Richardson, 2004) states that nearly 66% of all cyber-security breach incidents, in the 280 organizations who responded to the survey, were conducted from inside the organization by authorized users. Additionally, an overwhelming 72% of organizations reported that they have no policy insurance to help them manage cyber-security risks (Gordon et al., 2004). However, most literature in the area of cyber security has been focusing on threats and attacks caused by an outsider imposed on the organization’s network or systems (Magklaras & Furnell, 2002). Hamin (2002) defines insider threats as “threats from computer misuse within the workplace … [as] it is generally concerned with the harms committed by employees against organizations for which they work” (p. 106). He further elaborates that under this definition the term employees actually refers to current, former, and temporary workers, as well as other individuals with close knowledge of the computer systems of the organization. For example, such individuals may include consultants or independent contractors working for the organization, system maintenance technicians from outside vendors who maintain the organization’s network and/or systems, or suppliers (Hamin, 2002). Magklaras and Furnell (2002) provided a definition of the term misuse as “to use (something) in a wrong way or for a wrong purpose” (p. 63). By extending this definition, they defined IT misuser as an individual who is using the available resources in an unacceptable way and for an unapproved purpose (Magklaras & Furnell, 2002). Moreover, the term insider is not classified by the physical sense of the term, rather by its logical sense. As such, this study will define an
insider cyber misuser (or insider cyber attacker) as a current, former, and/or temporary employee (including consultants, contractors, suppliers, maintenance technicians, etc.) who is using available computing resources either from inside the organization’s networks or via the Internet in an unacceptable way and for an unapproved purpose in order to intentionally cause harm to the organization’s networks or systems. This definition is also in full agreement with the description of insider cyber attacker provided by the former FBI director, Mr. Freeh, in his congressional testimony on “cybercrime” before the U.S. Senate Committee on Judiciary, Subcommittee for the Technology, Terrorism, and Government Information (Freeh, 2000).

The Days Following the Cyber Attack...

Within one day of the cyber attack against KU’s e-learning system, faculty members and students mounted complaints to KU’s IT department and eventually to the institution’s president. During an emergency president’s meeting, Dr. Lopez demanded from Mrs. Rodriguez an immediate audit of the technology network and a comprehensive report about the status of the e-learning system, along with immediate actions to restore the system. Following the meeting, Dr. Lopez assured both students and faculty members that a ramification plan was underway to save the semester’s work and bring the e-learning system back to operation.

Mrs. Rodriguez solicited a proposal for a security audit from the IS consultant, Ms. Maya, who specialized in e-learning systems as well as crisis recovery management. Ms. Maya interviewed the IT director about the recent sequence of events, basic facts about the institution’s network components, and types of hardware/software comprising the e-learning system. The following day, Ms. Maya submitted a proposal to Mrs. Rodriguez that included details about the scope of a proposed audit, a general outline of the proposed audit process, and a projected timetable as well as a projected report about the network audit and status of the e-learning system. Several days following KU’s cyber attack, Ms. Maya was invited to perform the security audit.

During the audit phase that lasted a week, Ms. Maya visited KU’s campus several times. Some of her activities included:

- Interviews of numerous personnel from KU’s IT department and faculty members who have used the e-learning system as part of forensic computing. Also, interview Mrs. Rodriguez about past and present incidents with employees related to negative performance, low morale, or other employee behavioral issues.
- Visit to KU’s server farm in order to observe the network physical space, review relevant manuals, and technology-related documents provided by Mrs. Rodriguez, and perform some tests on the server hosting the e-learning system application.
- Perform a security audit on the server hosting the e-learning system application.
- Create a comprehensive report about the security audit outcomes.
- Create a two-phase comprehensive action plan and recommendations for further action based on two criteria: (a) mission-critical issues, and (b) non-mission-critical issues.

The E-Learning Security Audit Process

Goan (1999) discussed various issues related to cyber attack processes. He provided a set of recommendations which were followed in this audit process. He advocated the use of audit trains in which logs of system activities are reviewed. Additional audit mechanisms that Goan (1999) recommended include monitoring operating system commands: “Looking for hidden processes, checking log files, and testing for known backdoor passwords are among the multitudes of manual techniques that system administrators may engage in via available system commands” (p. 50). Sandhu and Samarati (1996) also proposed an audit methodology similar
to the one proposed by Goan (1999) that includes collection of data about the system’s activities to find traces of the intruder or perpetrator. Furthermore, Goan (1999) maintained that “evidence must be gathered and analyzed in a timely fashion so as to improve the chances of detecting an intrusion before significant damage is done or before the trail left by the intruder becomes cold” (p. 50). This recommendation is effective in enabling early detection of cyber threats before damage is inflicted, or before a threat materializes as an attack. Often times the cyber-attacker may survey the network over a period of time before setting up a malicious action (Hamin, 2000). Therefore, the audit methodology employed in this case also included collecting data about the system activities and analyses following the methodologies proposed by Goan (1999) as well as Sandhu and Samarati (1996).

The audit performed by Ms. Maya attempted to uncover the attacker’s activities after the fact. As in this case, cyber attack audit is often used to provide legal evidence to the court system (Hamin, 2000). Consequently, cyber attack audit mechanisms can be utilized forensically in order to apply severe penalties to criminals, rather than as a preventative measure (Hamin, 2000; Schneier & Kelsey, 1999). In line with the recommendations provided by Goan (1999) as well as Sandhu and Samarati (1996), a number of system tools, log files (event logs) and access control mechanisms were reviewed on the server hosting the e-learning system. The findings were reported to Mrs. Rodriguez and Dr. Lopez.

The Audit Results

The security audit findings and the two recommended action plans were presented by Ms. Maya, the IS consultant, to KU’s president, Dr. Lopez, and KU’s IT director, Mrs. Rodriguez, about two weeks following the discovery of a cyber attack against KU’s e-learning system. During an interview with Mrs. Rodriguez, it was revealed that the network administrator had been dismissed a few weeks prior to the cyber attack. Consequently, Mrs. Rodriguez was filling in the network administrator position. Not having had formal training in server and network administration, Mrs. Rodriguez did not maintain the current functions of the network. Although the former network administrator, Mr. Perez, had provided the administrator account usernames and passwords to Mrs. Rodriguez, no effort had been made to remove them from the systems—to change passwords or alter access permissions on the systems. Neither the server nor the network was protected by a firewall mechanism. The server farm did not appear to have a physical security system to its entrance. Servers were not securely attached to a server rack and server screens were not systemically locked down.

The server hosting the e-learning system application appeared to be unlocked on the system level. The http server application, Microsoft’s Internet Information Server (MS-IIS), appeared intact. The server operating system was functioning and appeared to be intact as well. During the assessment of the e-learning server, Ms. Maya was able to log in using the “admin” information provided by Mrs. Rodriguez, which was the same information as used by the former network administrator, Mr. Perez. It appeared that the e-learning system application had been uninstalled from the server (on the C drive) remotely. The whole C drive had only 2GB disk space, while three other partitions of the hard drive (F, G, and H) were found empty with 1GB of free space on the F drive and 2GB of free space on the G and H drives. There were backups of only two of the 84 courses, dating back six weeks, according to Mrs. Rodriguez. It appears that there was a tape backup software installed on the server, but no scheduled backup was set. There were records of several previous manual backups done up to a few days before Mr. Perez left KU.

Based on the account of Mrs. Rodriguez, there were approximately 84 courses using the e-learning system. Additionally, 42 faculty members were regularly using the e-learning system. It was unknown how many students were enrolled in these courses or had access to the e-learning
system; however, that information could be retrieved from the student information system that was running on another server and had not been attacked. The e-learning system application’s centralized user database was fully corrupted on the 8989 port, and could not be recovered. Additional observations included the server settings on port 8989 that were not configured properly and the administrator e-mail for errors, which was not configured at all. There was no license key set for the e-learning system on the existing server. Also, there was no virus scan or net shield on the server. It appears that there was no uninterrupted power supply (UPS) system on the server in case the power was to shut down.

An inspection of the server system log files showed numerous entries for the “admin” account logging remotely via the Internet. The log files also confirmed the suspicion that the user of the “admin” account had uninstalled the e-learning system application remotely and a timestamp for this activity was present in the log files. A trace of the IP number was performed to the source perpetrator who used the “admin” user. Based on this information, it was concluded that Mr. Perez, the former network administrator, was associated with the intentional cyber attack on KU’s e-learning system.

Following a massive search by Ms. Maya and the two technicians in KU’s IT department, several tapes of manual backups were found. Some of the backup tapes included specific backups of the e-learning system performed by Mr. Perez several weeks before his departure from KU. It appeared that these tapes included backups of the 84 online courses lost during the cyber attack. However, these backups had been done about three weeks prior to the day of the cyber attack. As such, if restored properly on a new e-learning system, three weeks’ worth of academic work (from the date of the backup to the date of the cyber attack) would be lost, aside from the delays and slowing of student productivity during the two weeks of the security assessment and recovery.

CURRENT CHALLENGES/PROBLEMS
FACING THE ORGANIZATION

Can KU Save the Term?

Based on the security audit and development of the audit outcomes report it was evident that KU was challenged to bring the e-learning program back on track. During a meeting with KU’s president, Dr. Lopez, and KU’s IT director, Mrs. Rodriguez, Ms. Maya expressed some reservations on KU’s ability to rebound quickly from this incident. She noted that it might take some time to develop an action plan in order to reinstate the e-learning system. Additionally, Ms. Maya, noted that it may take longer to order new equipment, receive it, install it, and bring it up to a production level. Moreover, the backups that were found for the e-learning courses could be restorable. However, these backup copies were several weeks old and would require additional time to restore. As such, KU was facing major challenges as part of their recovery process. What are the different action plans Ms. Maya can propose to help KU recover the e-learning system? What actions will be needed in the short run and what actions will be needed in the long run to help KU recover? Will they be able to save the current academic term?

Will KU Reorganize the IT Department?

It appears that KU’s IT department currently may lack the knowledge and skills needed to operate this department. Although understaffing of universities’ IT departments appears to be a major issue for small and medium higher educational institutions (Ross, Tyran, Auer, Junell, & Williams, 2005), KU’s current situation is not limited to staff shortage only. KU’s president, Dr.
Lopez, noted that a reorganization of their university’s IT department is indispensable. However, given the long history of KU’s IT director, Mrs. Rodriguez and her dedication to work, reorganization of the department may bring some new challenges both for Mrs. Rodriguez and Dr. Lopez. Additionally, Dr. Lopez does believe that Mrs. Rodriguez is a trusted and devoted employee. However, evidently her ability and skills to serve in the capacity of overseeing KU’s whole IT operation may be questionable. Moreover, the overall reputation of KU’s IT department was drastically eroded over the course of this incident. Furthermore, faculty members and students were discussing other potential failures. Concerns about privacy of students’ records were conveyed by the faculty senate to the president. Will KU’s president, Dr. Lopez, be able to reorganize the IT department without losing a trusted and devoted individual such as Mrs. Rodriguez? What policies and procedural changes will KU’s IT department need to undertake as a result of this incident? Will this incident impact other KU’s departments? Should KU file charges or seek legal actions against the former employee that conducted these acts?

The Lessons Learned

This case illustrates the importance of proper policies and procedures as well as proper IT knowledge by key individuals in the IT department of small universities. Moreover, although most attacks reported in the U.S. are performed by insiders, most of the security attention has been given in previous literature to attacks performed by outside perpetrators. This case addresses the issue of insider cyber attacks by providing some theoretical background on the term including clarification of the term “insider attacker.” This case also highlights the need for formal policies and procedures in the IT department. In order to avoid such devastating consequences, IT departments should have clear policies and procedures (e.g., ones provided by CERT.org or US-CERT.gov) for various threats as well as for attack types.

Finally, this case supports the need for academic institutions to engage in creating proactive security safeguards for e-learning systems. Literature already noted that academic institutions should develop strategies to overcome challenges unique to e-learning systems (Zhang et al., 2004). However, very few institutions actually do so due to various challenges. One of these challenges relates to the limited security of e-learning systems resulting from untrained IT personnel in academic institutions, as seen in this case study. Another challenge related to the limited security of such systems is the tight budget under which IT departments of some academic institutions operate. Often, academic institutions are “too busy handling day-to-day IT operations to devote [adequate] resources to disaster planning” (Ross et al., 2005, p. 47). Moreover, lack of proper funding to academic institutions’ IT departments has been causing IT directors to cut down on the number of qualified employees, that is, reduce overall staff, or hire unqualified employees. Levy and Ramim (2004) proposed eight key elements that are needed for successful e-learning programs. Three of these key elements are budget and funding, a high quality support and development team, as well as policies and procedures (Levy & Ramim, 2004). As this case study demonstrates, the consequences of limited IT knowledge combined with a lack of proper policies and procedures for IT-related issues such as employee discharge can be devastating to small academic institutions. Nevertheless, academic institutions should be open to embracing changes related to their current e-learning system’s security strategy even though they are renowned for their resistance to IT changes (Chae & Poole, 2005; Wang, & Paper, 2005).

ACKNOWLEDGMENTS

The authors would like to thank the editor-in-chief, Dr. Mehdi Khosrow-Pour, the accepting associate editor Dr. Ira Yermish, and the four anonymous referees for their careful review, constructive comments, and valuable suggestions.
REFERENCES


**ENDNOTES**

1 The name of the university discussed in this case is concealed due to the sensitivity of the issues addressed. A fictitious name is used.

2 Names of specific individuals discussed in this case are concealed due to the sensitivity of the issues addressed. Fictitious names are used.

Michelle Ramim is an adjunct professor at the Huizenga School of Business at Nova Southeastern University teaching MIS courses. She earned her bachelor’s degree from Barry University in Miami, Florida and received her Executive MBA from Florida International University. Ms. Ramim is currently finishing her PhD in information systems at Nova Southeastern University. In the past few years, she has been teaching varieties of on-campus, hybrid, and online management as well as MIS courses in several local universities. She is also an MIS consultant helping corporations and educational institutions on diverse information system implementations issues. Her current research interests include information systems success, online learning systems, e-learning systems security, and academic misconduct in e-learning environments. She has published in several conference proceedings, an invited book chapter, and encyclopedias. She served as a co-chair of the education track for the IEEE SoutheastCon 2005 conference. Ms. Ramim has been serving as a referee research reviewer for several national and international scientific conference proceedings and MIS textbooks. She is a frequent speaker at national and international meetings on management information systems and online learning topics.

Dr. Yair Levy is an assistant professor of management information systems (MIS) at the Graduate School of Computer and Information Sciences at Nova Southeastern University. Prior to joining the school, Dr. Levy was instructor and director of online learning at the College of Business Administration at Florida International University. During the mid to late 1990s, Dr. Levy assisted NASA to develop e-learning platforms as well as manage Internet and web infrastructures. He earned his bachelor’s degree in aerospace engineering from the Technion (Israel Institute of Technology). He received his MBA with MIS concentration and PhD in management information...
systems from Florida International University. His current research interests include value of information systems, value of online learning systems, e-learning systems security, IS and online learning effectiveness. Dr. Levy is the author of the book, Assessing the Value of E-Learning Systems (in press, by Information Science Publishing). His research publications appear in the IS journals, conference proceedings, an invited book chapter, and encyclopedias. Additionally, he chaired and co-chaired multiple sessions/tracks of his research area in recognized conferences. Moreover, Dr. Levy has been serving as a member of academic review board and a referee research reviewer for numerous national and international scientific journals, conference proceedings, as well as MIS and information security textbooks. He is also a frequent speaker at national and international meetings on MIS and online learning topics. To find out more about Dr. Levy, please visit his site: http://scis.nova.edu/~levyy/