An Evaluation of Privacy and Security Issues at a Small University

Michael Jones
North Carolina Agricultural and Technical State University
mejones@ncat.edu

Abstract

Colleges and universities process large amounts of personal information obtained from employees, students, and the general public. Such information includes income tax returns, employment history, salary, loans, and credit information provided by students and their parents. Additionally, data gathered from research, admissions records, medical files, and library access information are also maintained. Institutions of higher learning represent a large portion of the United States' network and computing infrastructure, which accounts for approximately 15 percent of all Internet domains [15]. Colleges and universities are major targets for identity theft because of the sizable amount of data that is managed and stored within these institutions.

The copious amounts of information that colleges and universities maintain suggest that security should be a top priority. How can higher education institutions protect personal and sensitive information of their students and employees? Most institutions focus on privacy and security for students; however, their employee's personal information is just as vulnerable to security invasions. This study will explore how a small university can decrease privacy concerns and security attacks against its students and employees.

Introduction

Institutions of higher education possess enormous amounts of employee and student personal information that needs to be protected and secured. Colleges and universities face potential security vulnerabilities because of the quantity of data that is processed and stored, ranging from lack of security policies to unsecured wireless networks [15]. The Privacy Rights Clearinghouse [10] indicates that since February 2005, more than 50 million people have had their personal information potentially exposed by unauthorized access to computer systems, which contained sensitive information. Furthermore, 50 percent of all reported security breaches have occurred at colleges and universities. With technology changing so rapidly, colleges and universities are finding it difficult to keep pace with advanced security procedures and privacy policies. Administrators at educational institutions must recognize that personal information can be maintained or disclosed in any manner, whether it is verbally, electronically, or in a written document [13].

Objectives

The objectives of this paper include the following:

- Identify securities and privacy strategies that are in place at a higher education institution.
- Explore different departmental privacy procedures.
- Conduct a security risk assessment to identity privacy and security vulnerabilities.
- Identify training procedures for faculty and staff in privacy policies.

Literature Review

U.S. government and corporations have responded to security issues by investing large amounts of money on information security. Higher education institutions in Canada, the European Union, and elsewhere are dealing with security and privacy issues under national data protection laws [6]. With the proliferation of identity theft, colleges and universities in the United States can no longer ignore the responsibility of privacy and security. Not recognizing the vulnerabilities in the current security systems can result in lawsuits and additional legal obligations. Institutions must move to more of a “need to have, needed to know, need to share, need to retain system” [6]. This system will help protect personal information and improve quality and efficiency of the data generated.

The Educational Security Incidents (ESI) observes all the information security incidents that occurred at colleges and universities worldwide that was reported in the news [13]. According to the year review for 2007, security breaches have increased, along with the number of institutions affected.

ESI Year Review	**2006**	**2007**	**Increase**
Total Number of Incidents:	83	139	67%
Total Number of Institutions:	65	112	72%

Total Number of Incidents by Type in 2007	
Theft	39
Penetration	30
Employee Fraud	1
Impersonation	3
Loss	12

One of the most recent university breaches was earlier this year (2008) at the Harvard Graduate School of Arts and Science, when a hacker broke into the web server. The server contained personal information on 10,000 applicants who applied for graduate school and graduate housing for the 2007 school year [2].

According to Privacy Rights Clearinghouse, there have been more than 2.5 million identities involved in security breaches from colleges and universities in the United States during the first six months of 2008 [10]. As the number of breaches increase, administrators must be aware and prepare the universities for these attacks.

In order for colleges and universities to address the security issues, a comprehensive information security assessment should be conducted to identify security vulnerabilities. This assessment should focus not just on the technology but the institution as a whole. College and university administrators must be cognizant of the myriad of ways that information can be illegally obtained and disclosed, including, verbally, electronically, or in a written document [13].

The mission of higher education institutions is to provide education, scholarships, and service to outside environments by being inclusive, diverse, and supportive of the local community [15]. Privacy and fairness are key values in higher education, since they allow the students and faculty the ability to open inquiries without having the subject to one's interests examined or scrutinized by others. The "purpose of security is to ensure the availability, integrity, and protection of information, services, networks, and computer systems" [1]. However, there is a conflict between providing security for students and faculty, while preserving the institutions' principals. Civility and community is core because they serve as a foundation for human respect that is essential for development of such policies and procedures. Ultimately, security within higher education must be molded to fit the academy's unique and delicate nature to maximize privacy, while maintaining integrity [15].

Barriers and Issues

Databases are more accessible now than years ago because distant learners, students, and professors are granted access to the network. The structure of university information technology systems is created on the system of free information exchange and to accommodate diverse user population [18].

In addition to being targeted by some very savvy hackers, college computer systems have been made vulnerable by the schools themselves through improperly trained employees who have access to the sensitive files [16]. For instance, a University of Delaware student allegedly changed her grades online, after impersonating a professor by finding his Social Security number online and guessing the password to the professor's computer. Software glitches and errors by staff members leave computer systems vulnerable for attacks [11]. Colleges have become a target of cyber-intrusion for several reasons, including the following:

- Half of colleges and universities use Social Security numbers as student identification.
- Students download music and videos.
- University databases house lots of personal information and have lax computer and network security.
- Around the clock access to administrative services and digital library resources contributes to potential malfeasance.
- The use of radio frequency identifications (RFIDs) and ID cards make universities an attractive target.

Approach

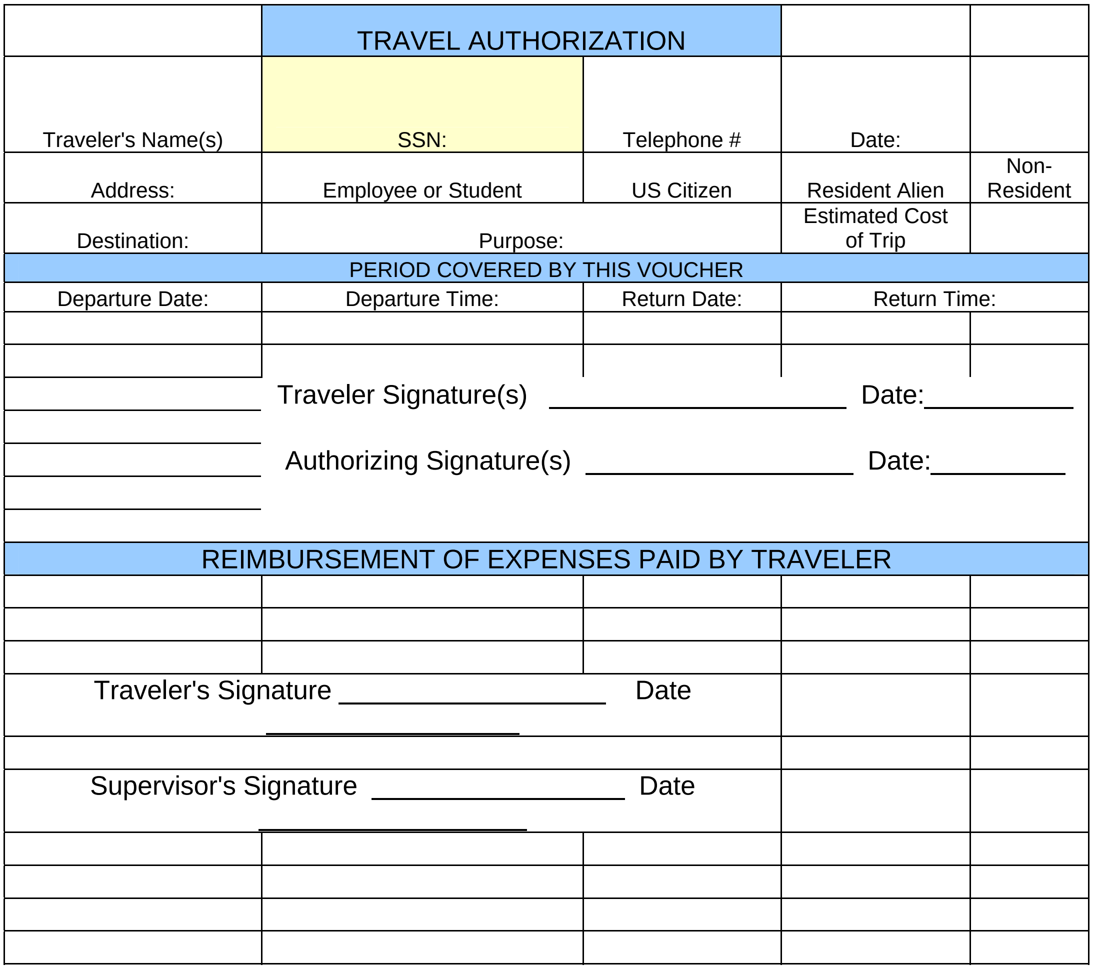
A qualitative approach was addressed to the privacy and security concerns at a small university. Data was collected in different departments in a natural setting. All forms that required a signature from students and faculty were collected from each department. Figure 1-1 is an example of travel authorization form. An interview with staff and faculty was conducted in regards to privacy and security concerns. Individual interviews, conducted using a structured questionnaire based on security and privacy, were collected from each department. These interviews were especially important for examining questions like, “How did the university train you as a faculty or staff member in privacy policies and security procedures?” Also, an interview with the information technology department was conducted to inquire about security breaches.

Results

Privacy and security strategies were in place but not fully implemented. The university is in the process of eliminating Social Security numbers as a form of identification; however, more than half of the forms required signatures with Social Security numbers. After interviewing the human resource department, it was found that each full-time employee that handles sensitive data must read and sign privacy documentation. However, there were no privacy and security policy documents in any of the departments. Employees hired within the past year who handle personal and sensitive information have not received any proper training on privacy and security. Therefore, sensitive data on an employee’s desk and computer screen can be viewed by anyone that is in the area. The results of the survey showed that most employees feel that they did not receive proper training on security procedures. Also, the majority of employees feel that there should be annual training that focuses on privacy and security awareness.

There were too many forms and documents that required signatures from different departments which, in turn, increased privacy and security threats. For example, the travel authorization form for a faculty member requires a signature from the chair of the department, dean of the school, Title I department, purchasing department, and accounting department. The sensitive information on the travel form will be viewed by five different departments, thus increasing security and privacy threats.

The information technology department routinely conducts a vulnerability scan, which is a good security strategy. Vulnerability scans are automated, network-based scans that attempt to determine network device types, configuration, and potential technical security vulnerabilities associated with each device [13]. In addition to vulnerability scans, the information technology department sets up a server with dummy files that are labeled Student Finances or Employee Records. The result of this action showed that there were security breach attempts internally, as well as externally. Overall, there was a minimal amount of security breaches at the university.



	TRAVEL AUTHORIZATION			
Traveler's Name(s)	SSN:	Telephone #	Date:	
Address:	Employee or Student	US Citizen	Resident Alien	Non-Resident
Destination:	Purpose:		Estimated Cost of Trip	
PERIOD COVERED BY THIS VOUCHER				
Departure Date:	Departure Time:	Return Date:	Return Time:	

Traveler Signature(s) ____________________ Date:__________

Authorizing Signature(s) __________________ Date:_________

REIMBURSEMENT OF EXPENSES PAID BY TRAVELER				
Traveler's Signature __________________ Date __________________				
Supervisor's Signature _________________ Date __________________				

Figure 1-1: Travel Authorization Form

Recommendations

Colleges and universities should develop an overall security risk assessment to identify security vulnerabilities and breaches in the institutions. A security risk assessment is an audit, penetration test, or vulnerability scan. The information technology department routinely conducts vulnerability scans and penetration tests, but an audit needs to be included. An audit will include reviews of documented policies, interviews, procedures, standards, and a review of security devices [13].

Information technology departments should use a proactive security approach to protect the computer environment. Intrusion detection tools alert you of attacks that have taken place; however, it does little to stop the attack from happening. Intrusion preventive tool software will not only identify the problem and alert you of an attack, but it will do something about the intrusion, such as change the configuration on a firewall to block an attack [9].

A training session on privacy and security should be developed and mandatory for all full-time and part-time employees, including student workers such as lab facilitators and teacher assistants. The training session should include a 30-minute video that shows security threats and privacy issues. Higher education administrators should view the security and privacy of students and employees as being as important as educating students.

Conclusion

With the increase of identity theft occurrences and the growing number of lawsuits due to privacy and security violations, colleges and universities must view security as top priority. These institutions are more vulnerable than corporations regarding security because of the accessible databases and because attention has not been placed in the area of securing personal information of student and employees. Staying informed about new technology and focusing on security awareness should eliminate chances on security attacks.

References

[1] Anderson, A. (2006). "Effective Management of Information Security and Privacy." *Educause Quarterly*, Vol. 29. Retrieved November 17, 2007, http://connect.educause.edu/library/abstract/EffectiveManagemento/39961.

[2] Bello, M. "Data Security Top Tech Issue for Colleges." *USA Today*. March 19, 2008.

[3] Brodie, C., Karat, C., and Karat, J. (2006). "Useable Privacy and Security for Personal Information Management." *ACM Volume*, Vol. 49, No. 1, pp. 55–56.

[4] Carlson, S., and Foster, A. "Colleges Fear Anti-terrorism Law Could Turn Them into Big Brother." *The Chronicle of Higher Education*, A31, March 1, 2000.

[5] Cassat, P., Salomon, K., and Thibeau, B. (2003). "IT Security for Higher Education: A Legal Perspective." Educause/Internet2 Computer and Network Security Task Force.

[6] Cate, F. (2006). "The Privacy and Security Policy Vacuum in Higher Education." *Educause Review*, Vol. 41, No. 5, pp. 18–29.

[7] "Data Privacy and Security for Higher Education Institutions." (2006). Global Compliance, http://www.globalcompliance.com/data-privacy-security-higher-education-institutions.html.

[8] Eaton, J. (2002). "Core Academic Values, Quality, and Regional Accreditation: The Challenge of Distance Learning." Retrieved November 21, 2007, http://www.chea.org/Research/core-values.cfm.

[9] Egan, M., and Mather, T. (2005). *The Executive Guide to Information Security*. Addison Wesley: New Jersey.

[10] Girard, K. (2001). "Security vs. Privacy. Retrieved November 19, 2007." *Nolo Press Privacy Right Clearinghouse,* http://www.baselinemag.com/article2/0,1540,13301,00.asp.

[11] Holub, T. (2003). "College Student Records: Legal Issues, Privacy, and Security Concerns." ERIC Clearinghouse on Higher Education. ERIC Identifier: ED480467.

[12] "Information Security: A Perspective for Higher Education." (2005). NEC Unified Solutions, Inc., www.necunified.com/downloads/whitepapers/Nec_higherEd_informationSecuritywhitePpr.pdf.

[13] LeVeque, V. (2006). *Information Security: A Strategic Approach*. John Wiley and Sons, Inc.: New Jersey.

[14] McCarthy, M.M. (2002). "The Supreme Court Addresses Student Records: Peer Grading Passes the Test." *Educational Horizons*, Vol. 81, No. 1, pp. 13–15.

[15] Oblinger, D. (2003). "Computer and Network Security and Higher Education's Core Values." *Educause Center for Applied Research*, Vol. 2003, No. 3.

[16] Salzman, A. "On Campus, a Security Card and More." *New York Times*, p. B14, October 5, 2003.

[17] Schevitz, T. "Colleges Leaking Confidential Data: Students Compromised by Internet Intrusions." *San Francisco Chronicle*, p. A1, April 5, 2004.

[18] Shaul, J. (2008). "Data Security and Higher Education." *SC Magazine*. http://www.scmagazineus.com/Data-security-and-higher-education/article/112517.

Biography

Michael Jones is currently an Instructor in the Electronics, Computer, and Information Technology department at North Carolina A & T State University. He teaches programming and computer applications classes. Mr. Jones has four years teaching experience and more than eight years of experience working for various companies.