Data Privacy and Security in Higher Education

BY TRACY WILLIAMS

As institutions review and strengthen their plans to secure confidential data, what proactive role does the human resource professional play as a strategic partner? Why are employees a critical part of the solution? And how are they educated regarding their responsibilities with data security? Datatel’s HR product manager shares some thoughts on this important topic. (CUPA-HR Journal, Fall/Winter 2003, Vol. 54 No. 3)

Introduction

Is your institution grappling with data privacy and security? Research shows that internal attacks are the most common type of data privacy violations, accounting for approximately 70 percent of all security breaches (Vamosi 2001). Knowing this, several precautions can be taken to protect confidential institutional data assets. One employee making a poor decision about his/her role with sensitive data can be costly—both financially and publicly. A recent survey by EDUCAUSE found that only 33 percent of institutions have security-awareness programs to instruct employees and students on the importance of technology security and their roles and responsibilities in this area (Carnevale 2003).

You may be thinking that this responsibility falls outside the realm of human resources (HR). However, strategic HR practitioners know that it takes a collaborative effort from all offices on campus to combat these serious threats. In fact, HR plays a critical role in data privacy issues and the prevention of security attacks and identity theft. Can the public trust your institution to secure confidential and private information maintained on employees, students, alumni, and donors? Let’s look at some actual examples of related events that have occurred in higher education:

- Without prior awareness of his background, an institution hired a convicted criminal (Smallwood 2003);
- Faculty, staff, and student e-mails were downloaded, and online banking activity was allegedly made viewable, by a student who compiled a database of personal identification information of approximately 4,800 members of the Boston College community—passwords, confidential access codes, credit card information, and Social Security numbers were published (Leyden 2003);
- A student was charged with stealing 55,000 names and Social Security numbers from a university database on training classes for staff members (Brulliard 2003);
- A contractor broke into a university computer network, causing an estimated $200,000 in damages (Read 2003).

There are also numerous potential threats to data privacy when employees:

- share system passwords;
- download files that have viruses, worms, spyware, or other harmful programs;
• do not log out of confidential systems at the end of the work day or when they step away from their desks;
• allow access to a controlled/secured area to a stranger or another employee who does not have authorized access;
• are not familiar with their roles and responsibilities (and consequences) with federal, state, and provincial laws and institutional policies regarding data privacy and security;
• attempt to gain unauthorized access to systems and data, often times seeking payroll and personal identification information for identity theft purposes;
• send electronic messages that create a hostile work environment.

The above examples illustrate just a few of the types of problems an institution might face if adequate data security measures and practices are not in place.

Data Privacy and Security Regulations
It is important to be aware of the many federal, state, local, Canadian, and European regulations when working with confidential information. Some of the more common regulations are described below followed by a Web site reference for more information.

**Health Insurance Portability and Accountability Act.** HIPPA provides several components, involving benefits eligibility, privacy, and security of a person’s protected health information, including notification requirements and privacy rules.  
http://cms.hhs.gov/hipaa/

**Electronic Communications Privacy Act.** This act mandates provisions for access, use, disclosure, interception, and privacy protections of various forms of wire and electronic communication. http://cio.doe.gov/Documents/ECPA.HTM

**Computer Fraud and Abuse Act.** This prohibits fraud and related illegal activities connected with computers. http://cio.doe.gov/Documents/CFA.HTM

**Family Educational Rights and Privacy Act.** FERPA protects the privacy of students’ education records, and applies to all institutions that receive funds under an applicable program of the U.S. Department of Education. This law does not cover employee records. http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

**USA Patriot Act.** This act grants law enforcement agencies access to previously confidential information to broaden their surveillance capabilities.  
http://www.lifeandliberty.gov/

**Graham-Leach-Bliley Act.** The Graham-Leach-Bliley Act applies to “financial institutions,” including institutions that obtain or use customer financial information and institutions that participate in financial activities, such as making federal Perkins loans or other types of “bank-like” activity with student debit cards for campus purchases.

Institutions that meet the definition of a financial institution must establish and implement a safeguard program to protect nonpublic customer “student” information.
Institutions that comply with FERPA comply with part of this act, but it is important to remember that FERPA only applies to students. This act applies to all individuals that conduct business with the institution. [http://www.senate.gov/~banking/conf/](http://www.senate.gov/~banking/conf/)

**Fair Credit Reporting Act.** The FCRA promotes the accuracy and ensures the privacy of information used in consumer reports through consumer reporting agencies for creditors and employers. [http://www.ftc.gov/os/statutes/fcra.htm](http://www.ftc.gov/os/statutes/fcra.htm)

**Privacy Act of 1974.** This act provides safeguards against an invasion of privacy through the misuse of records by federal agencies. [http://www.cftc.gov/foia/foiprivacyact.htm](http://www.cftc.gov/foia/foiprivacyact.htm)

**Identity Theft and Assumption Deterrence Act.** This law prohibits fraud in connection with identification documents made or issued by state entities. This only applies to public institution ID cards. Institutions should monitor any department that has document-making devices, and they should keep abreast of this regulation to determine applicability of this policy to the institution. [http://www.ftc.gov/os/statutes/itada/itadact.htm](http://www.ftc.gov/os/statutes/itada/itadact.htm)

**Personal Information Protection and Electronic Documents Act (Canada).** This act supports and promotes electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances by providing for the use of electronic means to communicate or record information or transactions. [http://www.privcom.gc.ca/legislation/02_06_01_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_e.asp)

**The Role of HR in Data Privacy and Security**
How does HR become part of the solution? There are eight key areas where HR can be instrumental in protecting sensitive information: (1) employee training, (2) background checks, (3) securing records, (4) appropriate use of the Social Security number, (5) creating reasonable policies, (6) contract reviews, (7) Information Technology (IT) collaboration, and (8) systems access.

**Employee Training**
Employee training is a key deterrent to data attacks, making HR a logical partner in reviewing policies and consequences of noncompliance. Effective training also includes sharing with employees and independent contractors their roles in establishing safe environments. Gina Salazar, HR manager at Riverside Community College, shares that, “Our employees are already familiar with the basics, but we want to make sure they have all the tools and resources to combat threats to our data systems, so we are revamping our training.”

Most data threats come from attackers who manipulate employee systems to hack into data or avoid technology all together to obtain physical records from a “secured” area. These attackers may be “trusted” employees, consultants, or disgruntled past employees. These individuals may have a high level of trust with some institution employees who could unknowingly share enough information with them to grant entrance to data systems or offices (Hiner 2002). These hackers are usually already
familiar with employer data systems and standard practices, and know the vulnerable security loopholes.

To combat this vulnerability, training should include: (1) educating employees on what types of behaviors and activities should be considered suspicious, and encouraging them to report such activity; (2) educating employees on what data or activities cannot be disclosed or conducted without consent; (3) educating employees on the consequences of failing to comply with data privacy and security policies; and (4) routinely testing employees’ knowledge regarding their roles within the realms of data privacy and security.

EDUCAUSE recently surveyed 435 institutions and found that changes in user behavior could prevent most security breaches of institutional networks (McElroy 2003). All employees should be informed about how viruses and hackers try to penetrate the institution’s systems and what they can do to prevent successful attacks.

In the end, the best defense in protecting an institution’s data is to provide employees, independent contractors, and students with proper training in data privacy and security issues.

**Background Checks**

Higher education tends to trust most applicants who are hired. Typically, if an institution conducts background checks at all, it is only for certain positions, or just to contact references. This is potentially dangerous, considering that internal employees conduct most data privacy and security attacks.

Mary Poquette, executive vice president for Compliance and Product Management with Verifications, Inc., a leading provider of background check investigations for employment purposes, says, “Of the background checks conducted by our company in 2003, nearly 33 percent had some type of factual discrepancy. Education information was falsified 23 percent of the time, criminal convictions were found 18 percent of the time, and employment history contained incorrect information 19 percent of the time.”

As institutions grapple with growing security regulations, more background checks will have to be conducted to demonstrate due diligence in providing a safe and secure environment for people and institutional data.

Deirdre Honner, manager of Employment and Compensation at Calvin College, says, “Background checks are an important part of the process in keeping our institution and assets safe.”

Equally important is ensuring the expertise and background of staff that have access to confidential data and systems. For example, making a serious hiring mistake in IT, Finance, or HR can be potentially disastrous to data privacy.

**Securing Records**

All hard copy records should be in a controlled access environment, and personnel file practices should be enforced. These practices will protect the institution if a claim or lawsuit is filed. Follow record retention schedules and be sure to maintain separate records where required by law. Separate records can be helpful if an institution is audited, and they can be used to provide limited access to confidential record data.
**Appropriate Use of the Social Security Number**

The best practice is to encrypt any computer transaction that involves a Social Security number. Institutions should not use a Social Security number for identification purposes across campus. The University of Texas at Austin is now a model for best practices, and according to their Web site, they are preparing a conversion of Social Security numbers to other unique identifiers after lessons learned with a public hacking incident (University of Texas at Austin 2003). The University of Pennsylvania took similar measures in appointing its first chief privacy officer in 2002—which was one of the first hired in higher education.

**Creating Reasonable Policies**

Do not take on more responsibility than the law requires. Write policies that directly apply to the data and security measures required by applicable laws, such as the Gramm-Leach-Bliley Act, FERPA, and HIPPA.

**Contract Reviews**

The contract review function may reside with the legal department, purchasing department, or risk assessment office. For institutions that do not have those resources, this responsibility often falls into the HR department’s territory, or it may in some cases be decentralized, with HR only playing a role. If contract review does fall within the realm of HR at your institution, make sure each contract the institution has with third-party providers complies with data privacy and security regulations. Regulations such as the Gramm-Leach-Bliley Act require that reasonable steps be taken to select and retain providers capable of maintaining appropriate safeguards for protected customer information.

At the very least, every institution should ask providers to confirm their compliance with applicable data privacy and security regulations. The Gramm-Leach-Bliley Act requires that contracts entered into before June 25, 2002, must comply by May 24, 2004. Contracts activated after June 24, 2002, should have been revised by May 23, 2003.

**IT Collaboration**

It is critical that all IT members have the training and resources required to maintain data integrity and security at each institution, and that there is IT oversight for protection of the institution’s assets.

Some institutions, such as the University of Texas at Brownsville, have an internal audit director to complete a risk assessment as part of a security audit and to uncover significant areas of concern where corrective action is required. Institutions that do not have resources for an independent internal auditor can utilize the expertise of their information management solution provider to provide independent and thorough audits.

An added benefit of using system providers is that they can recommend best practices on how to use their systems to protect your data, as well as your investments in those systems. For HR, confidential data should be restricted to those who have a “need to know.”
**Systems Access**
Exiting employees should lose access to the employer’s systems immediately upon termination. Regardless of the reason for separation, this important step should be standardized to demonstrate due diligence in protecting the institution’s assets. Make sure IT, HR, Physical Plant, ID Office, and other appropriate departments terminate all access immediately, instead of when it is “convenient.”

**Conclusion**
HR’s role in safeguarding employees and data should be a collaborative effort. HR is instrumental in strategic initiatives on campus that impact employees, customers, and the community. Minimizing the security loopholes will demonstrate due diligence and provide for a safer and more secure work environment that allows for strategic work to continue to accomplish the core mission of academic institutions, instead of spending time reacting to serious data privacy violations.

Alice Moore, manager of Administrative Systems at Wabash College, sums it up concisely: “Our campus balances these solutions and regulations with a collaborative approach between HR, IT, the Business Office, Financial Aid, and the Registrar’s Office. It is critical that our HR team is proactive in our efforts to reduce the likelihood of a catastrophic event regarding data privacy and security from an employee perspective.”

**TRACY WILLIAMS** serves as Human Resources product manager for Datatel, Inc., a leading provider of information management solutions for higher education. Her professional background includes more than ten years of human resource experience in both higher education and the private sector in managerial and consulting roles. She can be reached at (703) 227-1141 or taw@datatel.com.

**References:**


University of Texas at Austin. 2003. What is being done to protect Social Security number privacy at the university? https://www.utexas.edu/datatheft/ssnprivacy.html