Effective Management of Information Security and Privacy

Security and privacy are not IT issues—they demand a comprehensive, strategic, team approach to find effective solutions

By **Alicia Anderson**

In May 2005, hackers broke into Stanford University's Career Development Center, gaining access to Social Security numbers, résumés, financial data, credit card information, and government information for 10,000 students and recruiters. In the same month, 380,000 students, alumni, faculty, employees, and applicants of San Diego State University were affected when hackers broke into four of the university's business and financial services department servers, gaining access to Social Security and driver's license numbers. In January 2005, hackers broke into George Mason University's campus identity card server and gained access to the names, photos, Social Security numbers, and campus ID numbers of 59,000 current, former, and prospective students, as well as current and former faculty and staff.

The list goes on, and no university seems immune to these attacks. For many universities, such events have served as wake-up calls to develop a comprehensive information security and privacy strategy. This is no simple task, however. It involves balancing a culture of openness with a need for security and privacy.

Recognition of the diverse stakeholders—parents, students, applicants, alumni, staff, faculty, third parties—and their sometimes competing interests is both vital and difficult. Regulations, community expectations, ease of access to records, and increased cyber-threats demand an aggressive strategy while imposing sometimes heavy financial costs and cultural trade-offs. Effective privacy management and information security requires understanding both technical and human dimensions as well as acknowledging the need to address not only what is required (by law) but also what is expected (from the community).

Privacy and Security: Related, but Not Identical

Security consists of two primary components: physical and electronic. The campus police have clear responsibility for physical security. Information security refers mainly to protection of electronic data and networks, although information exists in both physical and electronic forms. Information security, from an operational, day-to-day standpoint, involves protecting network users from such cyber-attacks as phishing, spam, hacking, hidden code to make PCs into zombies,[1] and identity theft. It includes educating the user community in addition to providing technical tools. The central IT department usually handles this part of information security for systems under its control, but it does not control all information systems on campus.

Information security gaps exist within most universities for several reasons:

- No organized way exists to ensure appropriate security for systems outside central IT's control. In fact, departments have used security as justification for building and maintaining their own systems and networks, further promoting disparities in the level of importance given to security in the design of new systems.
- No organized way exists to provide security for information in non-electronic form, such as paper documents. Sensitive information is gathered on paper forms by various departments, with protection and security of this information left up to the policies of each department.

Although universities have taken the lead in research and training, a gap divides the state of academic security research and security operations in the university setting. Additionally, the academic culture often puts a lower priority on information security in relation to openness. Ced Bennet, emeritus director of Information Services at Stanford University stated,

> At a corporation where, for the most part, they want to keep information inside the corporation, they put up big fences. Universities, because they tend to be relatively open and invite inspection, tend not to put up fences. So it makes it even harder to manage the data which by law needs to be protected.[2]

To address information security at the enterprise level, some organizations have hired a chief information security officer (CISO), a relatively new position in most organizations. The CISO is responsible for providing tactical information security advice and examining the ramifications of new technologies. In most corporations the CISO reports to the chief information officer (CIO) or chief technology officer (CTO). The CISO role does not usually include responsibility for physical security, risk management, and business continuity, which are more often the province of the chief security officer (CSO), who has a broader focus and reports to the head of operations or directly to the CEO. A CSO typically has responsibility for global and enterprise-wide security, including physical security, protection services, privacy of the corporation and its employees, and information security. In other words, the CSO is responsible for coordinating all corporate activities with security implications.[3]

Privacy is even more complex than security, involving protection of sensitive data in both electronic and physical forms. Federal law recognizes no difference in the levels of protection expected for physical and electronic data. Privacy also involves protecting that which is personal, including an individual's body, belongings, and private life. Theft and stalking are clearly the responsibility of the campus police, but matters such as who should have access to the list of visitors to a dorm does not fall under their auspices. Other privacy matters that don't involve the campus police include access to e-mail and voicemail. Privacy is addressed by both policy and law.

There's an "expectation of privacy" at most universities. Gaps exist in definitions of what should be considered sensitive or personal. How to apply these principles in practical, operational terms challenges most universities.

Protecting the Sensitive

A privacy policy dictates who should know what. Policies and procedures supported by system enhancements can largely address protection of sensitive information, often identified or implied by federal laws or community expectations. Privacy is more important now because of linkages and access to data that weren't available before. Examples of potentially sensitive information include the following:

- Social Security numbers
- Grades
- Financial aid
- Research
- Donor information
- Health records
- Physical activity (such as garage or shuttle use)
- Student information
- Employee information
- Applicant information
- Credit card information
- Names
- Addresses
- Communications (who sends to who)
- E-mail content
- Network logins

Protecting the Personal

Protecting personal information has little to do with system automation, being primarily a matter of policies and procedures that govern human interaction. Privacy violations are not broadcasted or publicly disclosed but instead are reported to ombudsmen at many universities. Privacy concerns range from trivial matters to potential criminal violations. Examples include:

- Access to e-mail and voicemail
- Access to data on borrowed or loaned computers
- Access to an individual's desk
- Hacking
- Use of Social Security numbers on forms
- Salary questions
- Nosy supervisors
- Discomfort with undressing in certain areas due to physical abnormalities
- Inquiries about personal health
- Inquiries about reasons for time off
- Disability needs
- Stalking

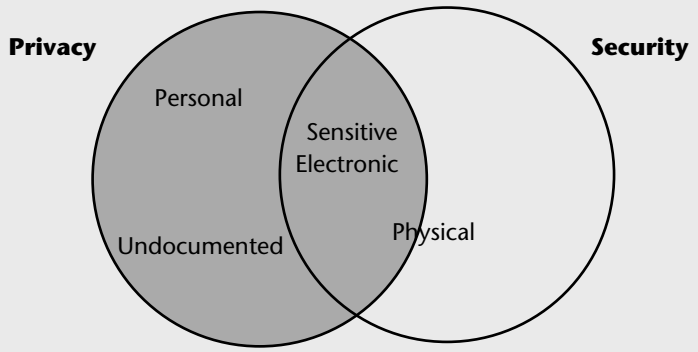
Parents, students, university staff, and faculty report these concerns. Often, a conversation initiated by the ombudsperson with the relevant party resolves these matters simply.

Privacy and Security Intersect

Several areas of concern are common to both privacy and security: policy establishment, communication, training and enforcement, procedures, detection/discovery of intrusions, notification of victims, and response to intrusions. Theoretically, security should protect privacy. However, they don't match perfectly—they overlap (see Figure 1). Security involves protection of the physical and virtual realms. Sensitive information in a form that could be accessed by others (such as paper or electronic

Figure 1

Relationship Between Privacy and Security



documentation) might be protected by security. Security measures typically do not protect those things that are personal and not documented, however. These matters should be protected by privacy policies.

The generally accepted role of information security is to support information privacy, but in some situations, one might be compromised for the sake of the other. For example, threatening e-mails might be accessed (a violation of privacy) to protect the security of potential victims. This interrelationship implies that one needs to be considered "superior" to the other, or at a minimum a plan established to decide which is more important.

Why Universities Are So Susceptible to Attack

Colleges have become a target of cyber-intrusion for several reasons. According to an article in *U.S. News & World Report*,[4]

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

The relatively new use of RFIDs and electronic ID cards exposes increasingly larger amounts of data to potential abuse, either by hackers or by authorized viewers. For example, data gathered about an RFID or ID card could be used to track an individual's habits, through stalking (a jealous colleague or friend tracking the person's location) or observation of a student's class attendance or eating habits (a parent tracking ID card use). Supervisors might monitor an employee's arrivals and departures by tracking the employee's ID card access to a parking garage. Some applications might seem reasonable, but who has the authority to decide access to the data and how it is used?

Besides technological vulnerability, universities suffer from human susceptibility. Privacy and security failures can result from errors, inadequate training, or malfeasance, made possible by poor controls on access. Frequently changing laws and inadequate processes to ensure compliance render universities ill-prepared to protect information security and privacy.

Make Information Security and Privacy a Priority

Several reasons argue in favor of universities focusing on privacy and security. First, the university and its constituents need a single source of accountability, responsibility, and ownership. Without this single contact, members of the university community don't know the person or department to contact with problems. As a result, issues either go unreported or are reported to several different parties who don't necessarily share information. Because no single person or group is aware of all the issues reported, the university risks not recognizing the magnitude of threats or responding appropriately. Each issue is handled in isolation and treated as an anomaly.

Universities must define who within their community has the leadership role in developing and implementing policies necessary to minimize unauthorized access to sensitive information. A single contact with the responsibility for assuming leadership in the event of an information leakage needs to be identified. This individual or body also needs to be responsible for electronic security. Someone needs to provide consistent information privacy and security leadership if many departments have their own policies and systems outside of a central IT organization.

Second, legal compliance calls for a focus on privacy and security. Several regulations require institutions to protect privacy. The Family Educational Rights and Privacy Act (FERPA) of 1974, for example, mandates electronic and physical protection of student information. Additionally, a privacy officer is required under FERPA. The Gramm-Leach-Bliley Act requires protection of financial data. Universities must comply with the Safeguard rule, which includes creation of a "comprehensive information security program." Health records are protected under the federal Health Insurance Portability and Accountability Act (HIPAA). There are still other legal obligations including compliance with European Union Data Protection Directive and other international laws; California and other state laws enacted to establish notice obligations in case of a security breach; and Federal Trade Commission regulations regarding electronic records.

Failure to ensure information security and privacy may result in financial and legal consequences to the university and individual representatives. Potential consequences include law suits from students, monetary damages for violations

of FERPA, loss of federal funding, and criminal and civil penalties.

Third is recognition of the community's expectation of privacy. University staff, students, and faculty have implicit assumptions about privacy that should be honored and, in some cases, formalized as policy. The university needs community-wide, articulated privacy standards.

Fourth, collaboration between business and technology is essential to provide an environment supportive of privacy and security. Business and technical leaders within the university should make decisions jointly, not in isolation. This is important because failure to collaborate results in inadequate systems and processes, and making changes is costly. Business leaders can use technology as a safeguard to help enforce policies. As new technologies and methodologies that protect privacy and ensure information security are discovered and proven by university research, the administration should lead the way in embracing and implementing them.

Fifth, a proactive (rather than reactive) approach toward ensuring appropriate privacy and security is urgently needed. Reacting to crises is not only ineffective and potentially negligent but also costly and difficult to recover from. The consequences associated with waiting to make changes only after an incident include loss of the community's trust, public embarrassment, loss of intellectual property, and identity theft. Universities need to establish systems, tools, and procedures to detect leakages proactively instead of responding to reports from the community. Establish policies and procedures to prevent violations of privacy expectations and regulations.

Sixth, systems should be designed to support privacy and security needs rather than redesigning older systems, which is difficult and expensive. One challenge is to achieve consistency across all departments, especially for systems outside of the central IT organization.

Seventh, focusing on privacy and security can protect against internal and external intrusion and abuse. Policies and system checks can prevent abuse from authorized users of information, while detection and prevention systems guard against unauthorized users.

Eighth, aligning security and privacy systems and policies with the best practices of other universities can put an institution at the forefront of the issue. Many universities are making significant policy and organizational changes to address information privacy and security, opening a great opportunity for leadership in this area.

Universities Act

Support for information security and privacy has come in the form of new positions and committees as well as policy changes. Universities are becoming more focused on best practices as their standard, as opposed to limiting their policies to those that ensure legal compliance alone. Investment in external consultants to assess vulnerabilities and make security and privacy recommendations is common.

Other changes include a growing number of policy offices and awareness programs, including steady growth in the creation of IT security officer positions in higher education since 1994. A common practice has been the realigning of the security functions and chain of command, with more enterprise-level than departmental officers. Per an October 2003 EDUCAUSE report,[5] 22.4 percent of universities have a chief IT security officer or equivalent, with 95 percent of those reporting to a senior executive administrator in IT and 50 percent to the CIO.

At the request of President Emeritus Charles Vest of the Massachusetts Institute of Technology, I conducted a study of 14 universities to determine how they approach the issues of security and privacy. The universities were chosen as representative of the larger population. They included large and small, public and private institutions. The participating universities took a variety of approaches to security and privacy needs on campus, from establishing privacy officers to committees to policies.

Privacy Officers

Privacy officers appointed for regulatory compliance are typically dispersed throughout the university. The privacy officers at five universities included in my study provide an interesting contrast in the approach to security and privacy on campus, with differing titles, levels of authority, assigned responsibilities, and key actions taken to date. In addition to the five described here, privacy officer positions on the other campuses included chief privacy officer, privacy compliance officer, FERPA compliance officer, and chief privacy/security officer for HIPAA.

Chief Privacy Officer. The chief privacy officer at one university reports to the vice president of audit and compliance. The part-time (three days a week) position has existed for three years and is supported by committees and working groups.

The key goals of the chief privacy officer include identifying university functions, routines, and business practices involved with privacy requirements and risks or remediation; developing a strong network within the campus community; identifying and accessing technology and resources available to assist in performing the assigned mission; and establishing an effective communication, training, and monitoring program. The privacy officer must also prioritize issues and determine the university components appropriate for privacy compliance, training, or remediation initiatives.

The chief privacy officer has acted to raise awareness on campus through a Web site, student records brochure, dissemination of a message from the provost's office, publication of guidelines for distributing and destroying information, presentations for students and staff, confidentiality statements, production of a brochure about ID theft, and training. The position manages information sharing with external entities and coordinates implementation of privacy policies or programs as mandated by federal law.

Associate Vice President for Institutional Compliance and Legal Affairs. This position reports to the president and is supported by a Social Security number

committee. The key responsibilities are to respond to privacy issues and problems. This associate vice president provides leadership for the Social Security number remediation project on campus.

University Privacy Officer. This part-time position reports to the chief financial officer and is supported by a staff of one (full-time equivalent). The privacy officer implements policies and procedures to comply with federal regulations and governs the treatment of individually identifiable health information.

Associate Vice President for Security and Privacy. This associate vice president reports to the CIO. The full-time position has existed for six months and is supported by a team of 14 people, with one person devoted to policy.

The position is responsible for ensuring the confidentiality, integrity, and availability of university data, information, communications, and services. The associate vice president and staff research, educate, assess, and consult in the areas of security risk, practice, policy, and technology. They maintain antivirus protection and offer site-licensed antivirus software to faculty, staff, and students. The associate vice president leads the university's identity management services and incident investigation and response.

The associate vice president played a major role in securing one university's wireless network (in the face of opposition) and installing firewall capabilities within academic schools. The provision of consulting services helped teach different groups how to secure their systems. Risk assessment provided security expertise to groups on campus to assess their infrastructure. Vulnerability scanning, patch management, centralized antivirus management, and training and education (mostly reduction of illegal peer-to-peer activity) were all provided. Policies were created, and the associate vice president took a leadership position in compliance.

Director of Information Technology Policy and Services. This part-time position reports to the CIO and has existed for 10 years. Responsibilities include establishing policy and granting permission to access personal data. The director created an appropriate use policy for the campus.

Privacy Committees

Standing and ad hoc committees are prevalent within universities, but few were established for the sole purpose of addressing privacy issues. Of the 14 universities contacted for this study, only two had committees devoted exclusively to privacy. One university has two separate privacy committees, one for senior executives and the other for representatives from each of the stakeholder groups. The committees are chaired by a member of faculty, the administration (for example, the deputy provost), or the privacy officer. The primary objectives include raising awareness, making privacy a priority, protecting Social Security numbers, and establishing privacy policies.

Security Officers

The effort to provide information security was led by an administrator in all 14 of the universities studied. The titles and responsibilities differed only slightly. All positions report to the senior IT executive with the exception of an information security officer who reports to internal audit. One-third of the universities studied separated the information privacy and security functions by appointing both a privacy officer and an information security officer. Half of the universities assign the responsibility for both information security and privacy under one individual within the IT department (typically the information security officer).

Security Committees

Half of the universities studied have committees devoted to information security. Some are as old as nine years and some as young as two. Although led primarily by the IT organization, they might be chaired by an IT representative, faculty member, or administrative executive. Primary goals include developing security policy, practices, and procedures; establishing a Web site policy; and determining guidelines or rules for directory and e-mail security. Additional committees address information security and privacy with a broader focus on IT in general.

Programs and Policies

Of the 14 institutions surveyed, 30 percent had formal security awareness programs. They used presentations, brochures, posters, postcards, and videos to communicate with the campus community. Programs demonstrated an increased emphasis on security outreach, education, and evangelizing. For example, they offered network authentication procedures as part of registration, video presentations and posters about virus protection, and security awareness seminars with faculty and staff on securing and protecting PCs and data.

A growing number of universities now have a Social Security number policy (eliminating them as student identifiers), Web site privacy policy, and an IT policy on security and privacy standards.

Recommendations for Action

A significant opportunity for improvement exists in the handling of information security and privacy within universities. Students, employees, parents, and alumni have expressed concerns with existing privacy and information security on campus. Security and privacy issues must be tracked and addressed at the policy level, and accountability for compliance must be clarified. Privacy and security policies should be created and widely communicated. Compliance with increasing regulatory demands related to security and privacy must be understood and kept current. Unless the handling of security and privacy improves, universities can expect increasing incidents of privacy violation, potentially generating adverse publicity, loss of funding, and lawsuits.

Security should be viewed as a means of implementing a privacy policy, but when these goals conflict, the university must have some way of establishing priority. Creation of a formal position or committee can help the community

make the right decisions regarding information privacy and security. The key areas an officer or committee will need to address are policy creation and enforcement, community education, and incident response handling.

Implementing the following recommendations would equip universities to handle information security and privacy appropriately.

1. Conduct Research

Many universities have assembled a task force to assess risks and areas for improvement. Potential areas for investigation include usage of Social Security numbers, community expectations for privacy, a resource audit (to determine whether the university has the system and human resources to adequately address privacy), and development of metrics to measure the effectiveness of information security and privacy programs.

2. Appoint a Privacy Officer

Create a privacy officer position to serve as a full-time resource exclusively dedicated to privacy. This person can address the diverse privacy issues that either are neglected or only partially addressed by different departments having no common policies or comprehensive reporting and tracking of issues. To ensure the goals of legal compliance and electronic security, this officer must build a strong alliance between the legal department and central IT. Individuals responsible for compliance with specific regulations (such as HIPAA or FERPA) should report to this person, who will provide general oversight of all privacy-related matters at the university. The privacy officer should be supported by designated compliance representatives as well as a privacy advisory board. This position should report to the president as a signal of the importance given to privacy and to ensure impartiality. A conflict of interest could result if the privacy officer reported to the IT or legal departments.

3. Establish a Privacy Advisory Board

Just as security experts exist, so do privacy experts. A group of experts and high-ranking representatives of the administration, academic departments, and the student body should be appointed to a privacy advisory board chaired by the privacy officer. The board should meet once a month, at a minimum, to proactively manage privacy at the university, including providing education and awareness programs to the community, reviewing regulations, establishing policies, and creating task forces to manage specific initiatives.

4. Establish an Insider Network of Privacy Advocates

Security is effectively addressed by IT systems and physical security teams. Privacy, however, requires many more manual adjustments in processes that must be performed by people. For maximum acceptance of privacy policies, tap into graduate students, faculty, and administrators with a passion for and expertise in this subject. These individuals could be used as researchers, privacy board members, or privacy advocates. Universities with successful privacy programs rely heavily on a network of liaisons inside each department who have a personal interest in privacy.

5. Launch Information Security and Privacy Campaigns

Create a culture where the community has the knowledge (what to do), skill (how to do it), and attitude (desire to do it) that support information security and privacy objectives. Security and privacy awareness must be part of an intentional, systematic, organizational change effort that adjusts attitudes and reshapes values and norms. These campaigns should be separate and led by the information security officer and privacy officer, with annual events to continually promote awareness and education.

Conclusion

Security and privacy are not the same, and the traditional functions of IT, human resources, and campus security do not adequately address the privacy issues arising on today's college campuses. Security receives organizational attention and funding, while privacy is largely neglected or assumed to be handled by existing security mechanisms. Institutions of higher education are naturally vulnerable to both security leaks and privacy violations because of their culture of openness.

Technology has enabled sophisticated capabilities for sharing information, but with attendant complexity and difficulty in protecting that information. Additionally, manual processes and practices persist, potentially leading to the compromise of sensitive information. Universities need new approaches to both privacy and security issues to successfully protect the personal information of their communities. *e*

Acknowledgments

Special thanks to the 14 universities that participated in the study and to the following individuals at MIT, who contributed significantly: Jerry Grochow, Tim McGovern, Laura Avakian, Hal Ableson, Simson Garfinkel, Joseph Ferreira Jr., Jeff Meldman, Mary Rowe, and Jamie Lewis Keith.

Endnotes

1. A computer implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner is called a zombie.
2. T. Schevitz, "Colleges Leaking Confidential Data; Students Compromised by Internet Intrusions," *San Francisco Chronicle*, Monday, April 5, 2004.
3. From the *CSO* magazine glossary, <http://www.csoonline.com/glossary/term.cfm?ID=970> (accessed December 5, 2005).
4. J. R. Marbaiz, "Lessons in Privacy," *U.S. News & World Report,* September 6, 2004.
5. R. B. Kvavik and J. Voloudakis et al., *Information Technology Security: Governance, Strategy, and Practice in Higher Education* (Boulder, Colo.: EDUCAUSE Center for Applied Research, Research Study, Volume 5, 2003), <http://www.educause.edu/LibraryDetailPage/666?ID=ERS0305>.

Alicia Anderson (Alicia.Anderson@sloan.mit.edu) recently completed the MBA program at MIT Sloan and resides in Cambridge, Massachusetts.