EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2006, Issue 17

August 15, 2006

Campus IT Security:

Governance, Strategy, Policy, and Enforcement

Richard Boes, California State University, Fresno

Tom Cramer, Stanford University

Vicky Dean, Cornell University

Roger Hanson, University of Wisconsin–Madison

Nan McKenna, Stanford University

4772 Walnut Street, Suite 206 ◆ Boulder, Colorado 80301-2538 ◆ www.educause.edu/ecar/

Overview

Sound information technology (IT) security policy and practices are necessary to protect the information assets of the university community, safeguard the integrity of institutional processes and the institution's reputation, and ensure compliance with federal and state regulations.

Traditionally, information security has often been viewed as an IT problem, but that viewpoint is increasingly outmoded in the environment of a modern university. Today's IT systems are used for a multitude of functions: they hold more data than ever before and are used by more people in support of almost every function and process—from student, human resources (HR), and financial and research administration, to academic research, course management and delivery, and everyday online life. In short, today's IT environment is an increasingly complex mix of systems, users, processes, and interdependencies.

In this new environment, pigeonholing information security as an IT issue is becoming less and less viable. Increased complexity and reliance on technology require ownership and action from all campus stakeholders to ensure an effective approach. Senior administration officials (data stewards, policy makers); central IT staff; departmental IT support staff; and the student, faculty, and staff end users of technology all have a role to play.

It is also not enough to count on technological approaches to meeting today's IT security challenges. Successful implementation of an effective "security blanket" also requires recognition of and action upon the cultural, political, and regulatory fronts of today's higher education institutions. While technology is certainly part of the solution—and many key emerging technologies show great promise for enhancing the security of our environments—there is no silver bullet that will achieve a secure campus.

New desktop management technologies are helpful only if the campus culture accepts notions of central control and if the populations we strive to protect agree to install them. Even moderately well-secured data centers and applications may pose an institutional risk if they don't comply with federal and state regulations. The most expert, experienced IT security team will be foiled in its efforts unless it has political support and governance that ensures sufficient funding, effective policies and operating procedures, and overall support from departmental and senior administration officials.

As increasing numbers of people in the academic community become active participants in IT security, it becomes difficult to maintain a holistic view of the security landscape. Administrators without a technology background can find the array of technical solutions mysterious and arcane. IT security staff must pay close attention to the realities of faculty and student culture, and campus leaders must keep up with the rapidly evolving set of regulatory requirements that, as much as anything, are driving security requirements and measures on campuses today.

This bulletin is based on the research of current IT security literature and on interviews with representatives from multiple campuses. While it does not provide a comprehensive solution to the myriad challenges facing campuses today, it does offer a broad survey of the current nontechnical issues facing higher education as it attempts to secure information assets and systems.

Highlights of Campus IT Security Drivers

The advance of technology is perhaps the most obvious driver of campus IT security. New systems emerge that both plug existing vulnerabilities and present opportunities for novel exploits. Yet technology is only one of many broad areas that drive the need and campus response for IT security measures. Three other critical factors that shape the security landscape in the university community are governance of security on the campus, the unique culture and values of higher education, and policy enforcement. Governance of security is a key internal issue that determines how, and how effectively, security measures will manifest themselves on a campus. Campus culture informs and frames all campus discussions and decisions about security, and it can be the most difficult area to resolve because of the apparent conflict between the traditional values of the academy and the implications of a tightly controlled IT and security environment. Legal drivers are the most obvious external pressures on security; the burden of federal, state, and other regulation is an ongoing reality in higher education.

Governance

By governance, we mean the considerations that go into the design and implementation of a campus IT security plan, from ownership and oversight to policy and practice. Senior leadership must take an active role in tackling the problem and generating institution-wide engagement, participation, and policies that support increased information security (Kvavik, 2003). Ownership and accountability, organizational structure, and funding are the key dimensions in governance.

Ownership and Accountability

Ownership and accountability for the security of campus IT systems include the formal selection of a person who is responsible and accountable, who has a large measure of authority for campus IT security, and who will create and disseminate security policy. For a variety of reasons, “IT security owner” is often not at the top of most people’s job wish list. Especially in institutions in which security has been a low priority on campus, owning responsibility and being accountable for IT security is generally perceived as a high-risk, low-reward job; failure is public, and success is personal.

Nonetheless, having a single owner who has both the accountability and authority for IT security is necessary to cut through departmental boundaries and diverse agendas. Clear lines of accountability and authority can help focus recovery efforts and avoid the finger pointing that can accompany a high-profile security failure.

Staffing and Organization

Operational responsibility for IT security functions within the institution is another key issue. Information security has generally been perceived in higher education as an area that “belongs” to IT organizations, leaving these organizations in the awkward position of attempting to enforce policy without a clear mandate or final decision-making power. Although IT groups typically have the depth and breadth of knowledge necessary to ensure proper IT security, even the best-resourced office is unlikely to be positioned to manage security for every application and system on campus, especially those run or administered by other departments and business units.

Ultimately, IT security depends on collaborative efforts among centralized and local resources. The overall design of the institution’s IT security structure should describe clear procedures and responsibility for incident reporting and incident handling, and it should include a comprehensive statement of responsibility for central IT, administrative business units, and academic departments.

Funding

The ongoing governance of IT security must include a structured funding model. Security is not free. Compliance requires staff to stay current with the latest information and tools, and it frequently calls for unexpected outlays for equipment or programs. Identifying appropriate levels of one-time and ongoing funding is critical to an effective security plan. Advocating for and receiving appropriate funding to fulfill a clear charge is one of the most important roles of the security owner and any supporting governance groups.

Higher Education Culture

A large enterprise faces a basic challenge in creating a balance between the information security risks it faces and the intrinsic values of that enterprise. This challenge can be particularly difficult in higher education, where core values can be at odds with the most expedient practices for implementing IT security programs. The academy tends to value community, autonomy, privacy, and fairness. These values often manifest themselves on campus through a culture of decentralization, resistance to standardization, celebration of academic and intellectual freedom, and the free and open flow of information associated with collaborative and cross-disciplinary research, teaching, and learning. Good security, on the other hand, is commonly implemented by fiat, using standard platforms, policies, and practices. It is engineered to provide accountability, auditability, and limits on access to and exposure of information.

Institutions that try to implement security policy in conflict with the core values of their community face an uphill battle. The character of security incidents has shifted over the last several years from events that affect a relatively small group or single system to events that affect thousands of systems and individuals. It is no longer sufficient to mandate tight controls on a small set of users or IT professionals to create an effective security blanket. Fundamental changes are needed in the way individuals approach electronic information and systems. Indeed, information security is everyone’s

responsibility. Changes in daily work patterns are needed to avoid or mitigate IT security incidents. For example, at the desktop level, individuals must run antivirus and antispyware software, configure firewalls, and update their system configurations on a regular basis.

Culture, because it is implicit and deeply rooted, can sometimes be the hardest campus security driver to understand, and it is often the most difficult to manage. Effective implementation of security policy, however, must factor in cultural considerations, adopting institutional values when they align with security needs and controlling for them when they appear to be at odds. Campus security programs can leverage students' proclivity for individualism and free software by purchasing enterprise licenses to offer free (to students, faculty, or staff) antivirus and antispyware software, as well as easy-to-implement desktop standardization. For example, from its Web site (http://iuware.iu.edu/), Indiana University offers IUware at no charge to all students, faculty, and staff. This service currently includes Microsoft Office Professional 2003, Norton AntiVirus Corporate Edition, and Firefox, along with an Indiana University Windows Authentication Update for users to secure their computers by turning off older authentication protocols. In a highly decentralized institution that places a premium on local autonomy, extra emphasis must be placed on communicating to and enlisting the local decision makers and departmental staff that will make or break any widespread policy implementation.

Policy and Enforcement

In the absence of a readily available IT security policy, the institution will be open to differences in approach, duplication of effort, and gaps in coverage. Policy must be set at the highest possible level, and it should be disseminated broadly.

Policies and Procedures

On a practical level, policy can be dry and uninteresting, and it can be challenging to ensure that faculty, staff, and students have read, understood, and complied with policy. It is as important to communicate and enforce policy as it is to create it and keep it current. Noncompliance represents an institutional liability—even for internally generated policies and procedures.

Statutory and Regulatory Drivers

The alphabet soup of regulations (FERPA, HIPAA, GLBA, SOX, DMCA), as well as state laws and industry mandates are, as much as any other force, driving the evolution of security measures on campus. The price of compliance is high; keeping up with regulations requires vigilant attention, prompt action, and implementation of new technologies, policies, operational procedures, and training programs. The price of noncompliance can be high, in terms of penalties; embarrassing exploits; and loss, corruption, or exposure of sensitive or confidential information (Salomon, Cassat, & Thibeau, 2003).

The advice of college or university legal counsel and policy officials is critical for creating a comprehensive, institution-wide program for the protection of electronic information

and resources. The sheer mass of online, regulated data, along with the ever-increasing number of applicable laws and statutes governing its use and protection, has created an environment in which tracking new laws, implementing the necessary responses to them, and monitoring ongoing compliance now requires a significant investment of campus resources—all under the rubric of information security. See Table 1 for a sample of protected data types.

Table 1. Protected Data

Record Type	Regulation and Description
Educational	FERPA, the Family Educational Rights and Privacy Act, protects student privacy by controlling the access, creation, and maintenance of student records. Individuals cannot bring a case against the institution, but the Department of Education can punish noncompliance by depriving an institution of federal funding. http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Medical	HIPAA, the Health Insurance Portability and Accountability Act, mandates a broad set of actions on the part of medical institutions; the parts that most affect universities (even those without medical schools or attached hospitals) are those that spell out the actions that institutions must take to safeguard the personally identifiable health information of individuals. HIPAA establishes the floor of privacy protection and does not preempt state action. In addition, individuals can bring an action, as well as the Department of Health and Human Services. http://www.cms.gov/hipaa http://www.educause.edu/ir/library/pdf/ERB0307.pdf
Banking	GLBA, the Gramm-Leach-Bliley Act, protects banking information (specifically, financial aid records but not student accounts). http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
Copyright	The Digital Millennium Copyright Act (DMCA) is designed to bring copyright law up to date with digital media. Universities must comply with the provisions of the DMCA for receiving and acting on complaints regarding the illegal use of copyrighted content using university resources. http://www.copyright.gov/legislation/dmca.pdf http://www.educause.edu/issues/dmca.html
Personal Data	The Personal Data Privacy and Security Act is federal legislation that protects personally identifiable data, defined as a name and at least one other piece of personally identifiable information like a Social Security, bank routing, or credit card number. http://leahy.senate.gov/press/200506/062905a.html The Payment Card Industry (PCI) standards and regulations went into effect June 1, 2005, requiring any institution that handles credit card transactions to take very specific measures to safeguard credit card data. Any leaking of credit card information from a university site can have dramatic impacts, up to and including termination of all card processing abilities by the banking industry at the university and financial liability for any fraudulent charges to stolen cards for 18 months. http://www.rsasecurity.com/glossary/default.asp?id=1093

What It Means to Higher Education

In order to build an effective security strategy, institutions must recognize nontechnical, security-related drivers on campus and may be forced to make difficult decisions spanning governance, policy, enforcement, security awareness, and the division of roles and responsibilities.

Many of these decisions are complicated by the culture and distributed nature of higher education. The basic notions of academic freedom and autonomy, a history of partial or full decentralization, the collaborative and cross-disciplinary nature of research today, and resistance to standardization all make higher education a particularly complex environment in which to implement an effective security strategy.[1] Leveraging and changing campus culture can be difficult and requires a long-term commitment and continual communication, but the nontechnical security drivers are critical to making any changes "stick."

At the same time, administrators need to account for these implicit but powerful cultural realities in any plans for designating an overall owner for security on campus, as well as the design of supporting organizations capable of setting and enforcing policy and carrying out security responsibilities.

Awareness

Education and awareness programs may be the single most effective way to sensitize the campus community to security needs and responsibilities. Lack of awareness is one of the leading barriers to effective security. If faculty, staff, and students don't know what they should be doing, in all likelihood they won't be doing it. Continual communication is required to address the rapid turnover of campus populations. In addition, different types of approaches are needed for different groups (end users versus system administrators) and audiences (Traditionalists, Baby Boomers, Gen Xers, Millennials). Cross-campus education programs typically encompass multiple media and outlets: informal briefings, departmental meetings, computer-based training, videos, group discussions, lectures, poster and banner campaigns, memo and e-mail pushes, and even awards.

Although higher education faces transient populations relative to industry, this does not need to complicate security management. Indeed, it can be an asset. Institutions can take advantage of student and junior faculty turnover and take the opportunity to orient the community to the latest shifts in the environment.

Leveraging relatively high turnover is one example of co-opting the particulars of university culture to create a stronger security campaign. Ultimately, any time spent assessing the unique aspects of the campus culture will be repaid with more effective implementations. Other strategies to raise security awareness include the examples in Table 2.

Table 2. Matching Strategies to Values

Campus Values	Strategies for Implementation
Collaboration and partnership within higher education	Look for opportunities to partner with peer institutions. Develop methods that will work across organizational lines; seek alliances within the campus and externally. Develop external alliances: National Science Foundation grants, Department of Homeland Security resources, National Institute of Standards and Technologies, National Cyber Security Alliance, and leading peer institutions.
Individualism and personalization	Offer various methods for learning and training. Link cybersecurity awareness programs to programs related to physical security for new employees and students. Know your students and their expectations. For example, provide a range of self-service tools to permit students and other to manage accounts and personal systems.
Accessibility	Support known, stable tools, and make reliability and ease of use a priority in security services.
Openness and transparency	Publicize incidents and attacks (both within the organization and in other institutions). This effort also can leverage a sense of community within the institution and among other institutions. It also conforms to some regulatory requirements to report security violations.
Community	Target specific groups; success can spread visibly and quickly as new practices are adopted by various communities.
Change	By its nature, higher education is a mixture of tradition and change. What is the motivation for people to make and support change, and is it sufficient? Be prepared to explain the reasons for change with concrete examples. There will be defensive responses. Be ready to wait to let people assimilate change.

Authority and Organization

A consistent message across the security literature is the criticality of identifying a single location for security ownership and authority. The preferred solution is the creation of a chief information security officer (CISO) function and a security office outside the IT organization. There is no consensus about reporting structure for the security office; the most effective placement depends on your institution's governance model. However, there is consensus that the authority of the office must be supported at the highest levels of the institution.

If it is not possible to identify a single person for security ownership, an alternative can be to create a strong governance group to oversee security policy and direction. Establishing a governance board with representation from the highest possible levels will increase awareness of security and provide an authority for policy enforcement. The security organization must have access to and/or involvement in the institutional planning process so that security issues can be considered holistically and be aligned with the institution's mission and goals.

Table 3 suggests roles and responsibilities to be covered in a security organization or organizations. Multiple roles may be handled by a single individual, if appropriate.

Table 3. Security Roles and Responsibilities

Role	Responsibilities
Security architect	Lead planning and implementation efforts; participate on security review boards; resolve issues and appeals.
Administrator	Implement security measures; participate in incident response.
Patch manager	Lead analysis and deployment of patches.
Audit lead	Respond to security audits; implement mitigation of audit findings; participate on security review boards *(see below)*.
Incident response	Oversee response to and clean up of campus security incidents.
Policy analyst	Maintain familiarity with statutes and regulations regarding IT security; communicate new requirements; serve as expert on requirements.
Outreach	Manage classroom or online training on security best practices and requirements.
Communication	Communicate to campus stakeholders; coordinate incident response communications; assist in communication of new requirements.

These roles are independent of the chosen organization structure. In a decentralized environment, a small central group coordinating efforts across distributed departments and led by a CISO can make an effective organization. The central group could provide the leadership and planning role in each area, with implementation and action taking place in each department or area.

In addition to a core team, consider creating a set of security review boards, with members from the security team and from other offices and departments. Suggestions for review boards from Burton Group (Cohen, 2005) include audit, technical safeguards, personnel, incident handling, legal/risk management, physical security, and campus awareness/training.

Security owners do not have to perform every security task on campus, but they do have a role in ensuring that appropriate measures are taken. Table 4 illustrates the responsibilities of a security governance structure by area.

Table 4. Security Areas and Responsibilities

Area	Responsibilities
Regulatory and statutory compliance	Stay current on new legislation and on updates and interpretation of existing legislation. Ensure that legal expertise is involved in interpretation and planning.
Data	Create and enforce policies that define practices regarding data access, replication, retention, and encryption.
Due diligence	Develop processes for audits of the campus IT environment and its security infrastructure.
Network	Create policies and best practices for intrusion detection, proactive scanning, and threat prevention.
Wireless	Create policies for appropriate use and authenticated access.
Workstations	Ensure that desktop computers have updates and patches, virus scans and protection, and malware scanning in place.
Physical safety	Lead the development of policies to prevent unauthorized physical access to computing equipment and storage media.

Finally, sufficient funding is critical to give the security owner(s) true authority to fulfill their mandate. Effective security requires appropriate resources for personnel, ongoing training, and equipment. Because of the rapid evolution of security threats, ongoing training is especially important for security professionals.

It is reasonable to anticipate at least one major unexpected security expense over the next few years and lay the groundwork for developing a contingency plan. When evaluating the appropriate level of funding, consider a case that includes the potential cost of not securing equipment, data, or the network, giving a worst-case risk analysis of possible security breaches with associated costs. Putting metrics into place to measure the cost and effectiveness of security measures, as well as the cost of responding to exploits, can assist in doing intelligent budgeting for the function.

Policy

Policy is the cornerstone of effective IT security. Two key drivers of policy are the determination of what is most important to keep secure and the level of risk the institution is willing to accept. Because security is a continuum that weighs function and access against risk, policies are effectively a contract with users defining the acceptable risk of behaviors and system design. Effective policies define the line between acceptable and unacceptable risk and the measures an institution will take to respond to the latter.

Creation and dissemination of security policy is a step that is easy to understand but hard to do effectively. Policy cannot be effective unless it is widely understood and enforced, so institutions should use a thorough process involving all stakeholders during its creation.

Security is rarely a top priority for students, faculty, or staff. Below are some best practices for the creation, enhancement, and dissemination of policy:

- Invite broad involvement in forming security policy so that final policies do not come as a surprise to key decision makers. Keep in mind that policy distribution is a chance to raise campus awareness of security issues.
- Develop a plan and a campus-readiness strategy for the dissemination of policy documents. Consider the different audiences and populations across campus in choosing ways to distribute materials.
- Large policy statements get lost when buried in communications designed to update administrative procedures. It can be helpful to create two levels of policy information with different target audiences: the institution's formal administrative policy, and a more informal, user-friendly guide to user security with emphasis on consequences.
- Setting an institution-wide calendar for regular security updates will help set expectations. At least three audiences should receive regular updates: key executives and faculty who control resources and influence opinion, end-users, and operational IT staff and their managers.
- Determine how often policies should be formally updated and distributed, considering the balance between updating too often and not often enough.
- Data owners should be designated for each piece of sensitive data. Obtain buy-in for interpretation from owners of data and other stakeholders, specifically, audit, legal, security, and finance.
- Ensure compliance through consistent planning that adheres to the university's interpretation of policy.

Key Questions to Ask

- What are the institution's most valuable information assets?
- To what degree is the institution in compliance with applicable statutes and regulations?
- In what ways do our security policies support our campus culture?
- How can we use our unique institutional culture to drive security enforcement?
- How can we empower departments to enforce security while maintaining strong central oversight?
- What is the governance model for information security at our institution?
- How do we measure security staff knowledge of applicable laws and statutes, especially where they intersect and overlap?

Where to Learn More

- Blum, D. (2005, February 24). *A systematic, comprehensive approach to information security.* (Vol. 1). Burton Group. Retrieved May 16, 2006, from http://www.burtongroup.com/content/doc.aspx?cid=656
- Davidson, M. A. (2005, January/February). Leading by example: The case for IT security in academia. *EDUCAUSE Review, 40*(1), 15–22. Available from http://www.educause.edu/LibraryDetailPage/666?ID=erM0510
- Information Security Governance Assessment Tool for Higher Education, developed by the Security Risk Assessment Working Group of the EDUCAUSE/Internet2 Computer and Network Security Task Force. Retrieved May 16, 2006, from http://www.educause.edu/ir/library/pdf/SEC0421.pdf
- International Organization for Standardization. (2005). Information technology—security techniques—code of practice for information security management. [ISO/IEC 17799:2005]. Retrieved May 16, 2006, from http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html
- Peterson, R., & Luker, M. (Eds.). (2003). *Computer and network security in higher education.* Boulder, CO: EDUCAUSE. Available from http://www.educause.edu/LibraryDetailPage/666?ID=PUB7008

Acknowledgment

This paper is the work of a cross-institutional project team participating in the IT Leaders Program, a leadership development initiative facilitated by MOR Associates, Inc., of Watertown, Massachusetts (http://www.morassociates.com/itlp.htm).

References

- Cohen, F. (2005, March 31). *Security governance for the enterprise.* (Vol. 1). Burton Group. Retrieved May 16, 2006, from http://www.burtongroup.com/content/doc.aspx?cid=660
- Kvavik, R. B., & Voloudakis, J. (with Caruso, J. B., Katz, R. N., King, P., & Pirani, J. A.). (2003). *Information technology security: Governance, strategy, and practice in higher education.* (Research Study, Vol. 5). Boulder, CO: EDUCAUSE Center for Applied Research. Available from http://www.educause.edu/ecar/
- Oblinger, D. (2003, March 18). *Computer and network security and higher education's core values.* (Research Bulletin, Issue 6). Boulder, CO: EDUCAUSE Center for Applied Research. Available from http://www.educause.edu/ecar/

- Salomon, K. D., Cassat, P. C., & Thibeau, B. E. (2003, March 20). IT security for higher education: A legal perspective. Boulder, CO: EDUCAUSE/Internet2 Computer and Network Security Task Force. Retrieved May 16, 2006, from http://www.educause.edu/ir/library/pdf/CSD2746.pdf

Endnote

1. An interesting look at academic culture and security is Diana Oblinger's 2003 research bulletin, which defines higher education's core values as community, autonomy, privacy, and fairness. Oblinger then looks at those values in light of the requirements of security to focus on the availability, integrity, and protection of data (see Oblinger, 2003).

About the Authors

Richard Boes (rboes@csufrenno.edu) is Director of Information Technology Services at California State University, Fresno. Tom Cramer (tcramer@stanford.edu) is Associate Director, Digital Library Systems and Services, at Stanford University. Vicky Dean (vrd4@cornell.edu) is Assistant Director of Systems and Operations at Cornell University. Roger Hanson (rlhanson@wisc.edu) is Assistant Director, Internet Infrastructure Applications at the University of Wisconsin–Madison. Nan McKenna (nmckenna@stanford.edu) is Director of Process and Account Management at Stanford University.