

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2003, Issue 6

March 18, 2003

Computer and Network Security and Higher Education's Core Values

Diana Oblinger, EDUCAUSE Center for Applied Research



Overview

Colleges and universities represent a sizable portion of the nation's computing and network infrastructure, comprising perhaps 15 percent of all Internet domains.¹ They face a host of potential security vulnerabilities, ranging from unsecured wireless networks to student-owned equipment to a lack of security policy and oversight. Because of the highly interconnected, international nature of higher education's computing and telecommunications infrastructure, vulnerability in one sector can be manipulated to cause damage elsewhere. Insecure computers and networks in higher education have been exploited, for example, to launch a variety of cyberattacks, both within the academy and in society.

In addition, campus systems hold a great amount of sensitive information about students, employees, alumni, and patients. Beyond such individual records, institutions must ensure that research, financial information, and course material are not abused or improperly accessed or modified. The computer and network vulnerabilities facing higher education translate into institutional risks including violation of federal statutes (such as the Family Educational Rights and Privacy Act [FERPA]), loss of reputation (and subsequent loss of funding), or compromised data (grades, transcripts, intellectual property, research results). Institutions that fail to effectively address these risks incur costs associated with the disruption of service and with recovery.

Although educators may agree with the need for security, differences of opinion arise when specific practices are adopted. For example, technical personnel may consider the use of a firewall a necessary precaution, while faculty might see this restriction on access as an impediment to intellectual freedom. Logging user access is one method of tracking intruders; however, monitoring and recording user access can be considered a threat to privacy. Finding the appropriate balance between security and the fundamental principles of the academy is challenging.

On August 27, 2002, Columbia University hosted an invitational workshop to establish a set of overarching principles that should guide any campus effort to establish security plans or policies. The goal of the workshop was to ensure that the articulation of higher education's values, particularly those affected by efforts to improve IT security, would guide colleges and universities as they decide how to improve the security of computers and networks. Based on research into principles articulated by a variety of academic groups, such as the American Association of University Professors and the Association of Research Libraries, and on statements by invited experts, the group proposed a set of six principles that higher education can use to steer its efforts to improve computer and network security. Those principles are civility and community; academic and intellectual freedom; privacy; equity, diversity, and access; fairness and process; and ethics and integrity. This was one of a series of workshops organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force and supported by a grant from the National Science Foundation.

Ultimately, each institution must determine which principles are most relevant and valued by its particular community. The principles proposed are not intended to bind institutions but to serve as a starting point for campus discussions about computer and network security. Security is necessary for higher education to be able to manifest its core values. Simultaneously, we must not imprudently implement security policies or procedures that undercut higher education's fundamental principles.

The purpose of this Research Bulletin is to highlight the importance of security and the principles that may guide many higher education institutions in their adoption. By illuminating both practices and principles, institutions can create an active dialogue that will help them find the appropriate balance between security and the openness that characterizes U.S. higher education.

Highlights of Higher Education Security and Values

Certain aspects of higher education make direct transposition of business or government security procedures a challenge. The unique mission of higher education and its role in developing individuals is one distinctive feature. Another is an operational environment characterized by a transient student population, a residential environment, and the research enterprise. These attributes create security challenges. Institutions grapple with balancing security and higher education's core principles.

Higher Education's Mission

Higher education's mission has been described as having three parts:

- *Education*. Transmitting, transforming, and extending knowledge, as well as promoting the intellectual and moral development of students²
- *Scholarship*. Discovery, integration, evaluation, and preservation of knowledge in all forms³
- *Service*. Furnishing special expertise to address the problems and needs of society

Higher education is thus devoted to a series of unique activities including human development, the creation and dissemination of new knowledge, and serving as a custodian and conveyor of culture and civilization. These activities, as well as higher education's core mission, result in a unique social contract between higher education and society.

Education clearly provides more than preparation for a career. Education is designed to provide social and cultural understanding for effective citizenship and the development of intellectual capacity to continue learning throughout life.

Higher Education Values

Several core academic values are potentially affected by the need for increased computer and network security.

Community

The academic community sees itself not only as a physical place but also as a virtual community and a state of mind. Colleges and universities view themselves as a community of scholars, instructors, researchers, students, and staff. The community ideal makes a campus the locus of learning, thoughtful reflection, and intellectual stimulation. In part, this notion implies that the community engages in its pursuits separately from day-to-day concerns.⁴

This community ideal informs the community-based governance of higher education. In shared governance, all relevant parties participate in and consult on decisions (typically faculty and administrators, but often other groups are involved as well). This localized decision-making culture tends to resist attempts by external groups to make its decisions or dictate policy or process.

Although the academic community may seem to be focused internally, the notion of community is also very broadly defined in higher education. Most institutions see their mission as serving a much wider community than merely the campus community. As a result, higher education has strong beliefs about inclusiveness, diversity, equitable access, international outreach, and support for the local community. Higher education accepts a responsibility to reach out with its knowledge, expertise, and culture to the external community.

Autonomy

Institutional autonomy may reflect the origins of U.S. higher education, in which institutions were intentionally independent of governmental control. Only in the last half century has public higher education become a dominant force. However, even in public higher education, institutions have adopted mechanisms (for example, governing boards) to maintain independence from government.⁵

That strong sense of autonomy is reflected at the faculty level in values such as academic freedom. Academic freedom embodies the right to pursue controversial topics, ideas, and lines of research without censorship or prior approval. American higher education steadfastly adheres to principles of academic freedom.

A closely related idea, though not synonymous, is that of intellectual freedom. Intellectual freedom provides for free and open scholarly inquiry, freedom of information, and creative expression, including the right to express ideas and receive information in the networked world.⁶ One possible interpretation of intellectual freedom is that individuals have the right to open and unfiltered access to the Internet.

Building on its history, higher education holds strongly to values of institutional and faculty autonomy. In such an environment, uniform standards for computer and network security may be difficult to reach.

Privacy

Both U.S. society and higher education place significant value on privacy. Privacy is essential to the exercise of free speech, free thought, and free association. The right to privacy has been upheld based on the Bill of Rights, and many states guarantee privacy in their constitutions and in statute law.⁷ Privacy, in the context of the library, is considered to be “the right to open inquiry without having the subject of one’s interest examined or scrutinized by others.”⁸ Privacy is considered a right of faculty and students, as well. For individuals to grow intellectually, they must be able to inquire, question, and challenge, knowing that their actions will be kept private.

Higher education defines fair information practices, including giving individuals notice regarding how information about them will be used. Higher education also guarantees that information collected will not be shared without permission. Among the implications of privacy is that computer and network users should have the freedom to choose the degree to which personal information is monitored, collected, disclosed, and distributed.⁹ In the context of libraries, borrowing records should be confidential. In addition, institutions must ensure the privacy of student records as well as other information, such as patient records, to meet federal requirements.

Fairness

Colleges and universities place great value on fair and predictable treatment of individuals. For example, institutions believe in due process.¹⁰ Higher education therefore defines processes and procedures, though they are not always the same as those of the external community. Equal access to information can also be seen as a logical extension of fairness. Equal access implies that users have the same access to information regardless of race, values, gender, culture, ethnic background, or other factors.

Higher Education Operational Environment

In some respects, higher education replicates the environment of a town or small city. There are residential environments, green spaces to preserve, roads and parking areas to maintain, buildings to operate, and utilities to be provided. There are few situations, outside of higher education, where students reside on campus. This residential environment creates computer and network security challenges. For example, students are able to bring their own computer equipment and connect to the network. The software on those computers can be from a host of vendors representing an array of versions, and both students and vendors might be unaware of security problems in those products. The transient nature of the student population creates additional security challenges, while the advent of wireless capabilities generates further problems.

Although not entirely unique, the instructional and research environments of colleges and universities are more pervasive and culturally situated than in governmental or

corporate training departments and research labs. Perhaps as an outgrowth of this environment, the academic culture tends to favor experimentation, tolerance, and anonymity—all characteristics that make it more difficult to create a culture of computer and network security.

Selected Security Practices

The purpose of security is to ensure the availability, integrity, and protection of information, services, networks, and computer systems.

- *Availability.* Computers, systems, and networks must be available on a timely basis to meet mission requirements or to avoid substantial losses.
- *Integrity.* Computers, systems, and networks that contain information must be protected from unauthorized, unanticipated, or unintentional modification.
- *Protection.* Computers, systems, and networks that contain information require protection from unauthorized use or disclosure.¹¹

A range of practices ensure security, a few of which are cited below. Some of these practices have the potential to raise concerns about their appropriateness in an academic setting. Colleges and universities face the challenge of balancing the need for security and the techniques available with their institutions' values.

Authentication. The use of a user ID and password is among the most straightforward of security approaches. However, password-guessing software (available on the Web) makes many passwords vulnerable. Can or should institutions enforce strict adherence to procedures, such as changing passwords on a regular basis or using complex passwords that include symbols, alpha, and numeric characters? If so, does this compromise autonomy?

Firewalls. Many organizations use firewalls to limit access to networks from the public Internet. A firewall prevents outsiders from accessing internal or private resources. Does this technique pose an unacceptable limitation on access to higher education?

Packet filtering. Packet filtering provides a passive means of security by allowing only packets that come from recognized sources or networks to enter the network. Does such a practice unnecessarily restrict access?

Virtual private network (VPN). A virtual private network establishes a tunnel between the user and the server. VPNs protect networks from unauthorized access and log user actions. Does the creation of a VPN unfairly restrict access to higher education's resources? Does the logging of a user's actions represent a violation of privacy?

Content filtering. E-mail can transmit sensitive information (such as patient or student information) and viruses. Institutions can install software filters to screen content, preventing intentional or accidental transmission of sensitive information. Does content filtering represent an inappropriate intrusion into privacy? Does it threaten intellectual freedom?

Web content filtering. Web content filtering programs allow organizations to track Web-based activities, such as students downloading music or video over the residence hall network. They can also detect the downloading of malicious code (often done by unsuspecting users). Are such programs a violation of privacy? Do they challenge intellectual freedom?

Logging. A common security practice is the creation of logs or records. Logs can include time/date stamps, time online, sites accessed, and so on. Is such logging an invasion of privacy?

Sniffers. Sniffer programs monitor and analyze network data with the goal of identifying problems. Sniffer programs can also capture network traffic and can read data in packets, as well as the source and destination addresses. Sniffers can be used legitimately (to identify network problems) or illegitimately (to intercept messages).¹² Could these programs stifle intellectual freedom?

Intrusion detection. Intrusion detection is based on finding atypical patterns in data and network traffic, which may be a sign of intrusion (someone making repeated attempts to log in using random passwords). Intrusion detection systems use network logs, and those who monitor the logs can deal with an attack by shutting off access or by “identifying a hacker’s dorm room and calling campus security.”¹³ Is this an invasion of privacy? Does it hamper intellectual freedom?

Biometrics. Biometrics is a security technique that uses physical traits (fingerprints, iris scans) as added security beyond user names and passwords or access cards. Some emerging systems target behavioral traits, such as how a person walks. Does biometrics invade individuals’ privacy?

What It Means to Higher Education

Computer and network security should not intentionally compromise the principles of the academy. In fact, without such security, there can be no privacy, and the principles and values of higher education could be jeopardized. As a result, each institution must find an appropriate balance among values, risk, and realistic safeguards. This balance will most likely be found by engaging the academic, technology, and security communities in a dialogue. The six principles identified by the workshop at Columbia University form the core of these discussions, which will identify implications that may lead to policies or procedures.

Civility and Community

Civility and community are among higher education’s core values. Respect for human dignity, regard for the rights of individuals, and the furtherance of rational discourse must be at the foundation of policies and procedures related to computer and network security. Communities are defined by a set of common values, common experiences, shared knowledge, and an ethical framework, as well as a responsibility and commitment to the common good. A tension often exists between standards of civility and the right to freedom of expression. Colleges and universities should identify

reasonable standards of behavior and acceptable, standard security practices and principles to support these core values.

Academic and Intellectual Freedom

Academic freedom is the cornerstone of U.S. higher education. It ensures freedom of inquiry, debate, and communication, which are essential for learning and the pursuit of knowledge. Faculty are entitled to freedom in classroom discussions, research, and the publication of those results, as well as freedom of artistic expression. In addition, individuals are entitled to seek, receive, and impart information, to express themselves freely, and to access material regardless of the origin, background, or views of those contributing to their creation. Intellectual freedom ensures information access and use, which are essential to a free, democratic society.

Although these principles are widely held among the professoriate, they may not be well understood by other groups, including technical personnel. As a result, all higher education personnel must be educated to respect academic and intellectual freedom.

Networks and systems must be sufficiently secure to prevent unauthorized modification of online publications and expression but open enough to enable unfettered online publication and expression. At the same time, colleges and universities, as repositories of information, must provide access not only to affiliated students, faculty, and staff, but also to other scholars and citizens.

Users must have access to information about system logging policies and procedures, including how log data are secured, de-identified or aggregated, and disposed of, as well as information about who has access to the log data, provided that such information does not jeopardize system security. Authentication and authorization systems that ensure compliance with license agreements should not retain individually identifiable user information. In addition, user authentication/authorization logs should be kept separate from system usage logs, with no linking of the two data sets.

Privacy and Confidentiality

In the United States, at least, privacy is the right and expectation of all people and an essential element of the academic environment. Confidentiality limits information access to only those with a need to know. For higher education, self-determination and the ability to make independent decisions depend on privacy. Confidentiality and protection of privacy is also required to comply with federal and state law. Privacy must therefore be protected in information systems, whether personally identifiable information is provided or derived. Higher education must strike an appropriate balance between confidentiality and use. For example, systems should be designed to enable only authorized access, while keeping the identity of authorized users confidential. These systems should respond to the privacy choices specified by individuals and should be able to implement fair information practices.

Equity, Diversity, and Access

Approaches to security and privacy should respect the equity and diversity goals of higher education by ensuring that access to appropriate information and the Internet is provided equitably to all members of the community. Not everyone interacts with computer or network-based systems with a common set of technical or personal resources. Minority-serving institutions, for example, may be particularly vulnerable to security attacks as a result of limited resources or a lack of in-house expertise.¹⁴ Technology must endeavor to enable all sectors of the community to participate in higher education.

Additional system demands imposed for the purposes of computer and network security should not unreasonably inhibit users whose purposes are legitimate but whose technology resources are limited. In addition, personal disabilities should be accommodated through secure systems. Accommodations for various groups of users should be kept confidential.

Fairness and Process

Access to computer systems, networks, and scholarly resources is essential for individual success within the academy. It is also essential for the delivery of quality services to students, faculty, and staff. Such access should be provided widely to every member of the enterprise. Colleges and universities must develop and communicate explicit policies governing the fair and responsible use of computer and network resources by the academic community. All policies should be accompanied by a description of the process to be followed when any member of the community violates the established policies. Institutions should revoke or limit computer and network access only as a result of a serious offense and after a defined process has been followed.

As a result, campuses must support core higher education values (intellectual freedom, privacy, civility) and not overreact to individual reports of abuse. Security policies, guidelines, and practices should be discussed and reviewed within the context of each institution's shared governance system. In the event of abuse, campuses must define due process for each member of the community, identifying the appropriate policy/office for guidance in handling incidents (copyright policy, campus posting, non-commercial use, and so forth). In addition, a breach in security should provide a learning opportunity so that future actions support, rather than undermine, security.

Ethics, Integrity, and Responsibility

Computer and network security depends on shared responsibility for the ethics and integrity of the campus community. Respect for confidentiality and privacy is necessary for the vitality of the community; the issue of computer and network security provides a tangible opportunity for teaching and modeling acceptable behavior, as well as reinforcing principles of fair and equitable access to electronic resources.

Inappropriate individual access or use of information infringes on both the rights and responsibilities of the entire community. All members of the academic community share a responsibility for security because disruption of services restricts the transmission and

exploration of knowledge. Ultimately, security based on integrity and ethics is stronger than security based on technology alone. All members of the academic community must be held to the same ethical standards.

Key Questions to Ask

Colleges and universities face a growing number of security challenges. The following questions may help institutions explore their options:

- Does our institution have a security policy? Is it clearly communicated to faculty, staff, administrators, and students?
- Do existing policies, procedures, and educational programs ensure that security is maximized? Does everyone on campus consider security a part of normal, day-to-day activities?
- How do we find the “right” level of security, one that balances ease and openness of access with protection from those who might cause harm to the institution?
- To what degree is it possible to change the behavior of a large, diverse community? Are individuals willing to take action to ensure security, or will a lack of behavioral change put the institution at risk? What role might education play?
- How do we develop support for the investments needed to guard against an “invisible” problem?

Computer and network security is necessary but must be implemented with sensitivity to higher education’s unique environment. Discussion among the academic, technical, and security communities will allow higher education to find the appropriate balance between historic principles and current computer and network security needs.

Where to Learn More

- EDUCAUSE/Internet2 Computer and Network Security Task Force, <<http://www.educause.edu/security/>>
- “Higher Education Contribution to the National Strategy to Secure Cyberspace” (July 2002), <<http://www.educause.edu/asp/doelib/abstract.asp?ID=NET0027>>
- American Association of University Professors, *Academic Freedom and Electronic Communications*, <<http://www.aaup.org/statements/SpchState/Statelec.htm>>
- American Library Association, *Intellectual Freedom Principles for Academic Libraries: An Interpretation of the Library Bill of Rights*, <<http://www.ala.org/alaorg/oif/ifprinciplesacademiclibraries.pdf>>

Endnotes

1. The National Strategy to Secure Cyberspace, September 2002, <<http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html>>.
2. Ernest L. Boyer, *Scholarship Reconsidered: Priorities of the Professoriate* (San Francisco: Jossey-Bass, 1990), p. 24.
3. James J. Duderstadt, *A University for the 21st Century* (Ann Arbor: The University of Michigan Press, 2000), p. 14.
4. Judith Eaton, "Core Academic Values, Quality, and Regional Accreditation: The Challenge of Distance Learning," <<http://www.chea.org/Commentary/core-values.cfm#values>>.
5. Ibid.
6. American Library Association (ALA), *Principles for the Networked World*, <<http://www.ala.org/oitp/principles.pdf>>.
7. American Library Association (ALA), *Privacy: An Interpretation of the Library Bill of Rights*, <<http://www.ala.org/alaorg/oif/privacyinterpretation.pdf>>.
8. Ibid.
9. ALA, *Principles for the Networked World*, op. cit.
10. Due process is not intended as a legal term in this context.
11. Rodney Petersen, "Accessibility, Integrity, and Confidentiality: Security Challenges for E-Business," 2002, <<http://www.educause.edu/asp/doclib/abstract.asp?ID=ebf0201>>.
12. See <<http://www.whatis.com/>>.
13. See <<http://www.cio.com/summaries/web/security/index.html>>.
14. AN-MSI Security Committee, "Developing Network Security at Minority-Serving Institutions: Building Upon the Title V Collaborative Effort Model," unpublished manuscript, 2002.

About the Author

Diana Oblinger (dianao@microsoft.com) is the Executive Director of Higher Education at Microsoft Corporation and adjunct professor at North Carolina State University. From October 2000 through 2002, Oblinger served as Senior Fellow for the EDUCAUSE Center for Applied Research.

Copyright 2003 EDUCAUSE and Diana Oblinger. All rights reserved. This ECAR Research Bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR Research Bulletin to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the author.