Chapter 1
IT Security and Academic Values

Diana Oblinger

Computer and Network Security in Higher Education

Mark Luker and Rodney Petersen, Editors

A Publication of EDUCAUSE

1

IT Security and Academic Values

Diana Oblinger

The networks and computer systems of colleges and universities abound with student, medical, and financial records; institutional intellectual property for both research and education; and a host of internal and external communications in digital form that are required for normal operations each and every day. Compromised computers on campuses have been used to attack other sites in government and industry. Maintaining a proper level of security for these digital resources is now a critical requirement for the institution.

Although educators may agree with the need for security, differences of opinion arise when specific practices are proposed. For example, technology personnel may consider the use of a firewall a necessary precaution, whereas faculty might see this restriction as an impediment to intellectual freedom. Logging user access is one method of tracking intruders; it also can be considered a threat to privacy. Higher education is faced with the need to apply appropriate security without compromising the fundamental principles of the academy. As a result, it will be important for colleges and universities to determine which principles are most relevant and valued by its particular community. Articulation of a common set of principles may serve as a starting point for campus discussions about computer and network security.

Unique Culture and Environment

Critical aspects of higher education preclude the wholesale adoption of business or government security procedures. The unique mission of higher education and its role in developing individuals is one distinctive feature. Another is an operational environment oftentimes characterized by a transient student population, a residential environment, and the research enterprise. A third is a widely held set of core values that shape the environment and behaviors of the community.

Higher Education's Mission

Three components are used to describe higher education's mission:

- *Education.* Transmitting, transforming, and extending knowledge, as well as promoting the intellectual and moral development of students (Boyer, 1990)
- *Scholarship.* Discovering, integrating, evaluating, and preserving knowledge in all forms (Duderstadt, 2000)
- *Service.* Furnishing special expertise to address the problems and needs of society

As a result, higher education supports a unique combination of activities that include human development and serving as a custodian and conveyor of culture and civilization. These characteristics result in a special 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 that will allow people to continue learning throughout life.

Higher Education Operational Environment

In some respects, higher education replicates a town or small city. There are residential environments, green space to preserve, roads and parking areas to maintain, buildings to operate, and utilities to be provided. This environment creates challenges for computer and network security. 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 and the adoption of wireless capabilities present further challenges.

Although not entirely unique, the instructional and research environments of colleges and universities are more pervasive and open than in government or corporate training departments and research laboratories. Perhaps as an outgrowth of this environment, the academic culture tends to favor experimentation, tolerance, and individual autonomy—all characteristics that make it more difficult to create a culture of computer and network security.

Higher Education Values

Several core academic values are potentially affected by the need for increased computer and network security. These include community, autonomy, privacy, and fairness.

Community

The academic community sees itself not only as a physical place but as a virtual community, as well as 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 (Duderstadt, 2000).

This ideal influences the community-based governance of higher education. In shared governance, all relevant parties consult on and participate in 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 internally focused, the notion of community is very broadly defined in higher education. Most institutions see their mission as serving a much wider community than merely that on campus. 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

Higher education's strong sense of 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 (Eaton, 2000).

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 (Eaton, 2000). 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 (American Library Association [ALA], 2003). 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" (ALA, 2002). Privacy is considered a right of faculty and students.

Higher education depends on 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 (ALA, 2002). In the context of libraries, borrowing records are kept 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 and therefore are invested in defining due process (ALA, 2003).[1] Because fairness and due process are priorities, higher education defines and relies on public policies and procedures that guide institutional behavior, even 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.

It is clear that computer and network security is now essential to protecting privacy and other academic values. It is just as important, however, that measures taken to improve security do not themselves compromise these values.

Principles for Implementing Security in Higher Education

In August 2002, the EDUCAUSE/Internet2 Computer and Network Security Task Force hosted an invitational workshop, sponsored by the National Science Foundation, to establish a set of principles that might guide campus efforts to establish security plans and 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.[2] Six principles were identified that may have implications on security policies and procedures.

Civility and Community

Civility and community are critical in higher education. As a result, 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, mutual 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 for the use of institutional networks, computers, and related infrastructure as well as 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. Faculties 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, express themselves freely, and access content 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 professoriat, they may not be well understood by other groups, such as technology personnel. As a result, all higher education personnel should 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 determine the degree to which they will provide access to other scholars and citizens, as well as to affiliated students, faculty, and staff.

Privacy and Confidentiality

In the United States, privacy is the right and expectation of all people and an essential element of the academic environment. Confidentiality limits access to certain types of information. Confidentiality and protection of privacy are also required to comply with federal and state law. To the extent possible, the privacy of users should be preserved. Privacy should be protected in information systems, whether personally identifiable information is provided or derived. Fair information practices should guide the collection and disclosure of personal information. 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.

Users should 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.

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 due to limited resources or a lack of in-house expertise (AN-MSI Security Committee, 2002). Technology should be used 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 should 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 should support core higher education values (intellectual freedom, privacy, and 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 and office for guidance in handling incidents (copyright policy, campus posting, noncommercial use, and so forth). Beyond dealing with security breaches, institutions should capitalize on the opportunity a breach represents to reinforce security messages and provide education so that future actions support, rather than undermine, security.

Ethics, Integrity, and Responsibility

Computer and network security is a shared responsibility, relying on 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 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.

Selected Security Practices

A wide range of practices can be used to improve computer and network security. Some of these practices have the potential to raise concerns about their appropriateness for an academic setting. Colleges and universities face the challenge of balancing the need for security and the techniques available with their institutions' values, and of discussing the relationships and tradeoffs with a degree of precision that can lead to acceptable, positive results.

- *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 by source.* 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.* A virtual private network (VPN) establishes a secure "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?
- *E-mail 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 invasion of 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 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) (Whatis, 2000). Could these programs stifle intellectual freedom?
- *Scanning.* It is possible to scan computers on a network to ensure that the machines have no viruses or vulnerabilities. Is scanning a computer without the users' consent an invasion of privacy?
- *Intrusion detection.* Intrusion detection is based on finding atypical patterns in data and network traffic, which may be a sign of intrusion (for example, someone making repeated attempts to log in using random passwords). Intrusion detection systems use

network logs; 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" ("Security," 2003). 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?

These and other questions may arise as a campus implements or strengthens its security plan. It is best that they be addressed in an open dialogue that recognizes the need for a proper level of security to protect academic values.

Conclusion

Colleges and universities face a growing number of security challenges. Institutions may begin to address these with well-defined security policies that have been clearly communicated to faculty, staff, administrators, and students. Policy alone will not suffice, though. Procedures and educational programs will be needed to ensure that security is as strong as is needed in relation to the risks. Changing the behavior of a large, diverse community can be daunting. Even more difficult is creating a culture in which everyone on campus considers 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?

Computer and network security is absolutely necessary but must be implemented with sensitivity to higher education's unique environment. Discussion among the academic, technology, and security communities will allow higher education to find the appropriate balance between traditional values and principles and current needs for computer and network security.

Notes

1. Due process is not intended as a legal term in this context.
2. 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, Association of Research Libraries, and Center for Academic Integrity, 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. 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.

References

American Library Association. *Privacy: An Interpretation of the Library Bill of Rights*. [www.ala.org/alaorg/oif/privacyinterpretation.pdf]. 2002.

American Library Association. *Principles for the Networked World*. [www.ala.org/oitp/principles/pdf]. 2003.

AN-MSI (Advanced Networking with Minority-Serving Institutions) Security Committee. "Developing Network Security at Minority-Serving Institutions: Building Upon the Title V Collaborative Effort Model." Unpublished manuscript, 2002.

Boyer, E. L. *Scholarship Reconsidered: Priorities of the Professoriate*. San Francisco: Jossey-Bass, 1990, p. 24.

Duderstadt, J. J. *A University for the 21st Century*. Ann Arbor: The University of Michigan Press, 2000, p. 14.

Eaton, J. "Core Academic Values, Quality, and Regional Accreditation: The Challenge of Distance Learning." [www.chea.org/Commentary/core-values.cfm#values]. 2000.

"Security." [www.cio.com/summaries/web/security/index.html]. Jan. 2003.

Whatis. [whatis.techtarget.com/definition/0,,sid9_gci213016,00.html]. 2002.