Chapter 7
Meeting the Cybersecurity Challenge

Ronald A. Johnson, Tracy Mitrano, and R. David Vernon

Organizing and Managing Information Resources on Your Campus

Polley Ann McClure, Editor

A Publication of EDUCAUSE
In the pervasively networked and ever more information technology–intensive world of higher education, cybersecurity has become a critical factor in protecting the integrity of institutional, student, alumni, research, and clinical data, transactions, and systems against what is now an era of continuous, automated, and increasingly intelligent and virulent cyberattacks. A comprehensive, institution-wide approach to information technology (IT) security, including policy, practice, and infrastructure, is the fundamental mechanism needed to protect campus operations from potentially devastating internal business interruptions, to guard against campus computer systems’ being exploited to launch cyberattacks against other sites, and to preserve the privacy of students, alumni, patients, and employees.

Security infrastructure is now also essential for the implementation of powerful and efficient e-business applications, shared digital library and electronic content environments, and the personalized relationship systems that many colleges and universities see as cornerstones of richer, customized relationships with their internal and external communities. These new strategic applications are directly dependent on an institution’s abilities to sustain effective security and to consistently deploy middleware campuswide. Often described as the technology superglue needed for the next generation of wide
area network–based applications and content, middleware provides services such as authentication (identifying legitimate users and software processes), authorization (determining what authorities or access someone or something should have), directories (repositories of information about people and resources), and integrated security, including important mechanisms that enable systems to decide whether to trust each other.

Meanwhile, campus approaches to IT security, and the closely intertwined privacy issues and questions, are telltales that will reflect, exemplify, and reinforce—or blunt, diverge, and detract from—an institution’s core values and ethics and its basic fabric of trust, trustworthiness, and public safety in cyberspace. In its approach to IT security and privacy, each institution will demonstrate by example, to everyone in its electronic family, what its values are regarding conduct in cyberspace and whether it can be a trusted network partner.

Unfortunately, cybersecurity threats are now growing faster than workable solutions, and much institutional practice in this area achieves little more than a false sense of security. At the same time, the implementation of middleware infrastructure across campuses is proving a challenge because of the intrinsic complexities of the software and architectures, as well as its dependence on scarce expertise that is difficult to extend into departments campuswide. Higher education surely does not need any more challenges, but these threats and opportunities are too strategic to defer or ignore.

**Threats to Cybersecurity**

Administrators and trustees of colleges and universities live under the abiding prospect of waking up to glaring media headlines about any one of a number of potential security breaches on their campuses: forged student records, release of personal financial information on donors, wholesale paralysis of a campus network or of e-mail or Web services, large-scale electronic embezzlement, identity theft,
destruction of databases, and even, with regard to the Health Insurance Portability and Accountability Act (HIPAA), litigation with potential criminal liability or stiff fines over unauthorized release of clinical information from, say, the student health center or a health science researcher's desktop computer.

Still another prospective nightmare for an institution is learning that some of its unprotected computer systems have been used, without its knowledge, to launch a major denial-of-service attack. In such an attack, potentially thousands of compromised systems overwhelm and disable selected targets, including those at commercial and government sites. When this occurs, if the institution has not taken reasonable steps to prevent exploitation of its computer systems, it is not only morally responsible but may also be legally liable for damages and threats to the security of the other institutions victimized in the attack. Because of the alarmingly large numbers of unprotected computer systems found on college and university campuses, higher education has been said to pose a threat to national security and the U.S. economy in this regard. This is another compelling reason to acknowledge the importance of protecting computers everywhere on campus, whether they are on faculty desks, in residence halls, in research facilities, or in public labs.

A third threat, much less visible but nevertheless important, is the opportunity cost of not being able to participate in future e-business, e-content, and relationship systems and initiatives due to the lack of the necessary security middleware infrastructure and the trust fabric that these new ways of doing business will be dependent on.

Higher education's security situation is difficult and getting worse. The sheer increase in the number of computers with institutional and other sensitive information and transactions, and the similar increase in the number of people with authorized access to them, greatly amplifies the traditional threats that people will misuse legitimate access and commit the traditional forms of computer crime like embezzlement and grade changing. This would be challenge
enough, but it is monumentally overshadowed by the exponential increase in other cyberthreats, such as pervasive automated snooping, hacking, and the propagation of viruses and worms.

How do these newer forms of cyberthreats occur? Cyberspace is now filled with many evolving species of automated probe-and-scan programs that may probe from a distance or nearby for computer server or PC configurations with security holes that have been left open. Such software scans and probes everywhere it can reach (and it now reaches almost everywhere) for even temporary security holes and other configuration weaknesses that can be exploited. If there is a weakness, even momentary, on any system in a network, it can be found and then exploited with no obvious sign of malicious entry or use.

On the average university campus, huge numbers of servers and personal PCs are set up and maintained (or perhaps not maintained is a more accurate characterization) with unlocked doors that in essence invite exploitation. Each can, and often does, infect and threaten other systems. Even at small colleges, hundreds of computers in residence halls might well be unprotected.

Where security holes are discovered, malicious software is automatically installed. Sometimes that leads to an immediate attack or vandalism, password or information theft, or data modification or destruction. But often malicious software is left to watch and collect more data, such as passwords and log-on IDs, which perpetrators use to get direct access to business, financial, student record, payroll, patient, trade secret, or alumni systems and transactions. Being able to steal the right password and log-on combinations can yield a gold mine of illicit access if the person with that log-on ID has access to key IT or other systems.

Some malicious software waits in hibernation for a signal to be part of a denial-of-service attack. Such attacks can cripple the targeted site’s network or e-mail services or a given set of servers for hours or days, cause the loss of messages and data, and bring campus, hospital, lab, or departmental operations to a standstill.
Even e-mail and simple Web access have become major vectors for the spread of dangerous worms, viruses, Trojan horses, and other malicious software. Every desktop or portable PC or personal digital assistant (PDA), and soon data-capable cell phone, is now a potential incubator of, launch pad for, and target of probing and snooping, cyberattacks, cybercrime, and ultimately cyberterrorism. These threats come from everywhere on the globe, now apparently including governments and crime syndicates, but experience shows that an alarming number are spread (and too many conceived and launched) from within a campus itself. But even if no attacks or malicious software ever came from within, they cannot be effectively walled out, because a college or university’s networks are necessarily somewhat porous to the rest of higher education and to the world outside. And in any case, colleges and universities simply cannot operate in a world in which they block external e-mail traffic and Web access and thus prevent staff and students from using their own computers and PDAs with other networks (from which they can and in many cases will pick up malicious software).

Weakness Links and Collective Vulnerability

A frightening reality for campus and higher education–wide communities, with cultures dedicated to openness and access, is that within them, almost everyone is dependent on everyone else for cybersecurity and privacy. We all are threatened by single points of security weaknesses in our campus neighborhoods.

The one person who fails to lock the door on a server can undermine the thousands who do. One Typhoid Mary has often infected an entire department, campus, or system. For example, if the bad guys can capture or compromise a person’s (say, the payroll manager’s or departmental chair’s) credentials on a poorly managed or open desktop system or server, that may be able to be used as an illicit entry point into a well-protected payroll, academic personnel, financial aid, or other system. The connectedness, collaborations, and
shared cyberspaces that are core values and products of higher education are, at the same time, and especially when supercharged by high-speed networks, powerful vectors for spreading malicious software and for magnifying its sweep and effects.

Unfortunately and unsurprisingly, most of the worst cases of university attacks and compromises occur at what is typically the weakest link: departmental, rather than central or enterprise, systems. Given that a campus’s weakest links potentially compromise everyone and everything at the institution, what can be done?

Institutions need to have departments, principal investigators, and all individuals whose computers are attached to the network comply with efficacious institution-wide security and privacy policies and procedures and for everyone to administer their systems intelligently and responsibly. That is a tall order with some punishing politics, some serious resource as well as support and training needs, and some very painful trade-offs.

The Common Good: Reinventing Partnerships

In higher education and elsewhere, the paradigm shift from time-shared central host computers to personal computers (and from central mainframes to departmental or group minicomputers and now servers) brought about something of the technology equivalent of the Protestant Reformation. No longer were faculty, staff, and departments largely dependent on the dispensations and expertise (and controls) of computing center gurus for their systems. Instead, individuals could freely choose their own brands of technoreligion and system management philosophy (or not), guided mostly by their own goals, expertise, and localized cost-benefit trade-offs.

In general, this shift to a model of widely distributed (and typically personally controlled) computers, along with mostly departmentally or group-controlled servers, enabled a huge step forward in empowering faculty, staff, clinicians, and students and in boosting the productivity and expertise of the community. In large, complex
universities, it also shifted much of the institution’s technology resources, and the control of and responsibility for systems management, to departments. This shift to a decentralized model was in part enabled by and dependent on the relatively small amount of expertise that used to be required to deal with a personal computer or small local area network (LAN) in a fairly innocent early era of networking.

But times have changed, and this departmentalized model is breaking down in dealing with security and middleware requirements, as well as other key technology and environmental changes. Today, dealing effectively with and maintaining the required skills for managing PCs, servers, and LANs on high-performance internetworks in the face of continuous security threats requires considerably greater expertise and skills and sheer amounts of time than straightforward PC or LAN management did before. Computer security in a networked environment has become an arcane and complex (but now universally needed) art, practiced in a constantly changing landscape, and typically requiring highly specialized staff who are dedicated to maintaining those areas of expertise.

Few general systems administrators, including those at departmental levels, are able to cope adequately with these responsibilities while keeping up with the changing technologies of their own departmental computer platforms and applications. And even if departments had the money to hire cybersecurity experts, it is unlikely they could be recruited to and retained at departmental-level positions. The challenges and expertise required to sustain competitiveness in the cyberinfrastructure and IT toolkit in any discipline is in itself usually a difficult and arcane job demanding exceptional subject area and technology expertise. Expecting people with such complex and demanding positions also to sustain up-to-date skills on cyberthreats, related security measures, and countermeasures for a multiplicity of computer systems is at best wishful thinking. Making matters worse is the reality that serious cybersecurity is a goal that is not seen as a relatively high priority at departmental levels.
The same is typically true for the software and standards components of the middleware infrastructure required for campuswide (and in some cases interinstitutional) e-business, e-content sharing, e-learning, and customized portal and relationship applications. Here, analogous to the earlier implementation of TCP/IP (Transmission Control Protocol over Internet Protocol) and the Internet protocol suite across campuses (which often had to displace proprietary departmental LANs forcefully), there is a strategic institutional requirement to establish interoperable middleware tools and consistently employed middleware conventions on a campuswide basis.

The development of such middleware will require a comprehensive effort not only on the part of central IT organizations but across campus departments and higher education institutions at large. This effort will take an unprecedented degree of national partnership, and in many cases it will also require institutional leadership courageously insisting on compliance and accountability for the larger institutional good, in an effort that in leading institutions parallels the effort and political capital and will that were required in the early 1990s to deploy Internet protocols and displace departmental and discipline-oriented alternatives. Internet2 and EDUCAUSE are active and effective leaders in coordinating higher education’s middleware evolution and in catalyzing deployments that include most leading research universities as participants (see www.nmi-edit.org/ and middleware.internet2.edu/).

What Institutions Can Do

Comprehensive security programs with strong and conspicuous leadership must be integrated into an institution’s culture and values, policies and priorities, network architecture, and operational functions. The following sections suggest a number of principles on which to base a comprehensive campuswide approach to IT security.
Understand the Culture and Values of Your Institution

A well-founded strategy for network security begins with an understanding of an institution’s culture and values. Although a number of critical practical issues are at stake, the issues of security and privacy are ultimately questions not of technology, procedure, and process but of human and organizational values, ethics, normative behavior, and the needs of the overall community. Following are some typical questions that need to be raised in this area:

• How does your institution feel about the privacy and accuracy of the information it holds about alumni, students, prospects, research subjects, patients, employees, and others?

• What are your institution’s views on acceptable use or abuse of university resources, including institutional data, when that use or abuse takes place in cyberspace? What are the citizenship obligations of interacting in cyberspace?

• How much does your institution seek out and value people’s perceptions of it as responsible and trustworthy?

• Does the approach to security and privacy reflect core institutional values?

To these questions, one might attach a corollary:

• Do IT policies and practices at your institution reflect those values? If not, how could they be made to do so?
Establish a Locus of Responsibility for IT Security

With the recent surge in security incidents and the likelihood that this represents a long-term trend, campus IT security has become so urgent that strong consideration should be given to the designation of officers or offices to address security and privacy matters from a campus perspective and provide a clear locus of responsibility for dealing with IT security incidents. Designating such an officer or office creates an implicit contract with the campus community; that is, with the services the officer or office provides comes the promise that the campus community will respect the authority of that officer or office. This is crucial, because that authority may entail decisions that have an impact on usage and administration. For example, the decision that a security officer makes with respect to blocking a problem source of traffic might mean disabling an individual’s or even a department’s or whole building’s network connection.

Campuswide understanding and consensus is the best means to make this approach effective. Associated groups and offices such as the regents or trustees, police, judicial administrators, audit, IT policy, campus policy, legal counsel, central IT organization leaders, and departmental IT representatives, not to mention faculty and student advisory boards, should be involved in the process of establishing the mandate for such an office. Stakeholder buy-in and campuswide education about the importance of IT security accrues in the process.

Establish Policy as an Executive Priority

Serious state-of-the-art security and privacy policies that cover the entire institution (not just central units) are an imperative component of an effective security strategy. But having, and broadly and repeatedly communicating, strong executive support is an equally critical ingredient. Some important questions to ask about policy and the policy process at your institution include these:
• Does your institution have such policies? If not, why not?
• Is there a policy development process? If so, is it centralized, decentralized, or hybrid?
• Is there conspicuous executive leadership and sponsorship of policy, or is this left to the chief information officer, auditors, or administrative staff who cannot get this job done alone?

The answers to these questions are important for knowing how to promote security and privacy policies and enforceable rules. If there is a centralized policy office, its vetting and buy-in processes can be used to formulate and promulgate institution-wide security and privacy policies. If there is not a centralized policy office, the creation of security policies can be used as a vehicle to establish either a policy office or its virtual mirror, that is, a group of the most senior executive administrators to initiate the process and sign off after engaging appropriate constituencies to review and critique the policies. (See Chapter Six for a discussion of the complexities of the policy development process.)

Take an Institution-Wide Approach

Institutional security and privacy and the data and information integrity that support them are dependent on the campus’s weakest links. Everyone is to a degree dependent on her or his colleagues to in effect lock the doors. And in many institutions, departments hold as much sensitive personal information on people as do central units. Do institutional policies and priorities actively extend to all departments, subdepartments, and individuals, including students and external users? Is there policy in place requiring both central and departmental units to keep known holes in servers and desktops closed?

The goal of the IT security program should be to make every user (individual and department) in the community own and be responsible for IT security. Because of the overwhelming technical
scale and basic human nature factors of security risks, a successful program will depend on achieving this goal.

Although it is important for all departments and individuals on campus to accept responsibility for security, it is equally important not to underestimate the need to orchestrate, moderate, and lead such efforts campuswide. Uncoordinated implementation of campus IT security strategies by well-intentioned but insular members of the larger community can create not only a false sense of security but a service cacophony capable of undermining the security sought by the whole. For example, installation of network firewalls may interfere with not just network performance but the integrity and capabilities of the network and university-wide security infrastructure itself. And even seemingly good things like the data encryption of critical university information can become a security nightmare if the university has not implemented a campuswide policy addressing the escrow of encryption keys.

Enforce IT Policies

Security and the implementation of security infrastructure (including middleware) are not likely to be seen by everyone on campus as an essential good that they need to be willing to make sacrifices to ensure. To have any hope of establishing and sustaining a reasonably responsible, durable, and future-oriented cyberenvironment, it is essential to have credible enforcement with real teeth. In the security and privacy realms, that means detection, investigation, and in some cases personnel actions or even criminal charges against not just staff but faculty, clinicians, and students. It can also mean unilaterally disconnecting problem computers and LANs and subnets from the network.

Make Security a Component of Network Architecture

Cybersecurity and privacy exist in the intersection of exceedingly complex technology, policy, and procedural domains that often must
accommodate local institutional variations. For an effective approach, an institution needs to have an overall conceptual and technical framework that provides a guiding architecture.

Security can be implemented more or less effectively in many ways in a well-designed IT infrastructure. Some institutions attempt to secure the entire enterprise network through perimeter protection, such as firewalls, but these perimeters are easily breached or circumvented though mechanisms as simple as e-mail attachments, and they do not protect from the considerable internal threats that institutions face. At the same time, they often impart a false sense of security that can be more dangerous than having no security at all.

All servers attached to the network should be made secure through passwords, authentication and authorization, properly configured and patched operating systems, virus software, and so forth. All personal computers should be maintained with appropriate antivirus software and system patches, and, if attached to the network directly, personal firewalls may be necessary for all. In special cases where warranted, the packets traversing the network between truly secure end points could be further secured by encryption, although this is a technique mostly relevant to data under protection of federal legislation, such as educational or health records, and traffic involving passwords and log-on IDs.

Colleges and universities must envision and apply an IT security architecture that encompasses the spectrum of their IT resources. And they must forge that architecture with the assumption that the Internet and virtually all campus networks are now, and will always be, insecure. With the acceptance of the inherently insecure nature of IT and rejection of the simple notion that gating campus communities from the world is the solution, there is a good chance that higher education institutions can effect positive change and protect crucial data, transactions, and other resources.
Educate and Train the Community

Adequate security is dependent on having well-trained and continuously informed security technology specialists, well-trained and informed systems administrators and IT staff, and well-informed computer users who understand the basics (and they easily can!). In addition to dedicated cybersecurity staffs, some institutions set up and actively market broad security and privacy training programs, sometimes including student orientation on security and privacy issues. Effective campus programs similarly have strong incident communication mechanisms that alert system administrators and users campuswide of threats, break-in attempts, and newly detected exposures and related fixes. Furthermore, policies that suggest that all users have some level of responsibility for campus security promote education as well as best practices.

Handle the Basics

Even the best and brightest technologies and middleware assemblages are often easily defeated by the reality that people do not always handle passwords and log-on IDs (and even “challenge-response” smart cards) responsibly. Nearly all relevant security infrastructure is based on simple authentication, that is, doing well at knowing and confirming who the person is who is seeking to use the technology resource. Simple but sometimes fatal breakdowns occur when people share, let their PC remember, or allow others to eavesdrop on password and log-on ID information. Unless there is sustained focus on education and enforcement of fundamentals of password and log-on ID handling and responsibilities, even the most sophisticated security and privacy architectures will be defeated.

Similarly, major progress is possible by establishing mechanisms (including inducements and sanctions) to universally install and maintain virus scanning software, to regularly install security software patches on PCs, and to ensure that known holes and exposures are closed on all servers.
Identify and Protect What Is Important

Well-run institutions have formal procedures for identifying and evaluating the mission-critical nature and sensitivity of systems, applications, and data and for ensuring appropriate controls and disaster recovery mechanisms are in place (see Chapter Eight for a discussion of business continuity). Similar assessment and action are needed from a security and privacy standpoint so that priority can be given to providing extra protections for the most sensitive or critical security and privacy exposures and needs. For example, materials protected by federal and state law, such as student records and soon all medical records, should be accorded high levels of security planning.

Critical information, transactions, and computers must have their own tightly managed and monitored security systems that will protect them in the event other security mechanisms like firewalls fail or are circumvented. This means configuring and managing them to survive attacks. Sometimes critical systems are also gathered in safe-harbor physical and network spaces that have significant extra monitoring, protection, response, and recoverability.

Focus First on Prevention, Then Cure

It is typically a lot less expensive to prevent security breaches than to heal them, and unfortunately more and more security problems are leading to largely incurable consequences. For example, how do you get the trust back from alumni (or get the trust of prospective donors) whose personal financial information has been stolen or inappropriately released and used by others for identity theft? Similarly, under HIPAA, failure to take customary preventive actions may be cause for a finding of negligence, maybe even criminal negligence. Given the public effects of such a finding regarding an institution’s handling of student health records, what would it take to make the institution (and the victims) whole? That said, a coordinated incident response process can be crucial to containing...
damage and learning and communicating lessons learned in what is typically a highly teachable moment.

**Be Skeptical of Protecting by Firewalls Alone**

Even if one tried to build electronic moats around departments or campuses, intractable problems would occur. Firewalls fail, and there will be innumerable back doors that will be vulnerable if the only protection is a firewall. Because firewalls cannot practically be configured to block all file transfer, e-mail, and Web use, they cannot provide sufficient protection. And in any case, building a moat around the campus does not help deal with the significant threats from within.

Kevin Mitnick, a convicted cybercriminal and break-in artist in cyberspace, says, “It’s naive to assume that just installing a firewall is going to protect you from all potential security threats. That creates a false sense of security that is worse than having no security at all” (*eWeek*, 2000). No matter what your institution’s view of firewallled perimeters is, it is important to ensure the protection of the end point systems in the event that firewalls are circumvented or an attack or threat comes from within.

**Proactively Detect and Probe**

Effective institutions perform automated campuswide probes of end systems to detect problem systems and vulnerabilities before the bad guys do. Such probing is an important internal campus tool to discover security exposures and react before they create problems and also to help educate and remind the community of the importance of security and to establish a sense of accountability and shared responsibility.

To be truly effective, these sweeps need to include all systems on campus, including those in departments and research groups and in the possession of individuals. When probes are used and offending systems are discovered, security personnel must have the executive
and institutional support and political backing required for them to remove those systems from the campus network.

**Identify and Implement Best IT Security Practices**


**Conclusion**

Maintaining the necessary level of security in the IT infrastructure of higher education requires a substantial commitment on the part of each college and university to educate its academic communities about the importance of computer and network security, rally the necessary financial and administrative support, promulgate effective policies, and create sophisticated network and security architectures sensitive to both security and service needs. Higher education relies on the security and integrity of data, transactions, and computers. It is not an option to allow the bullies, criminals, and now terrorists on the Internet to win the security wars.

**Note**

1. President George Bush has directed the development of a national strategy to secure cyberspace to ensure that the United States has a clear road map to protect an essential part of its infrastructure. The EDUCAUSE/Internet2 Computer and Network Security Task Force, established in August 2001, is supporting this effort by
Exhibit 7.1. Effective IT Security Practices

- Employ skilled, dedicated security and middleware staff
- Have a well-conceived security and privacy policy framework and architecture that covers the entire institution
- Proactively scan, probe, report, and follow up
- Quickly and broadly communicate newly discovered exposures, viruses, and incidents
- Aggressively enlist the aid of internal and external auditors
- Enforce IT policies; have accountability and consequences
- Distribute and universally require the use of secure application protocols and desktop virus programs
- Employ two-factor authentication (for example, smartcard plus password) for sensitive or critical systems and functions
- Move critical or sensitive systems to specially configured and closely managed server sanctuaries
- Employ campuswide mechanisms to ensure timely upgrade of desktops to more secure operating system releases
- Apply security patches to browsers and applications
- Use end system (including not just servers but also desktops) firewalls
- Garner the resources needed to support security strategies
- Offer training programs to ensure sufficient basic awareness throughout the institution
- Understand and position trust fabric and culture as the positive values and opportunities they are
- Build out interoperable middleware infrastructure
- Engage users, system managers, and policymakers in keeping systems safe campuswide
identifying short-term actions and long-term projects to address systems security problems in higher education. For details, see www.educause.edu/security/.

Reference

eWEEK, Sept. 28, 2000. [www.eWEEK.com].