Higher Education Contribution to National Strategy to Secure Cyberspace

July 2002

Submitted by the staff of EDUCAUSE
on behalf of the higher education community.
For further information about this report or the
EDUCAUSE/Internet2 Computer and Network
Security Task Force, contact Rodney Petersen
at 202.872.4200 or rpetersen@educause.edu
or visit http://www.educause.edu

Table of Contents

Higher Education Contribution to National Strategy to Secure Cyberspace July 2002

Executive Summary

The higher education sector plays an important role in the cybersecurity of America. Through its core mission of teaching and learning, it is the main source of our future leaders, innovators, and technical workforce. Through research, it is the basic source of much of our new knowledge and subsequent technologies. And finally, as institutions, colleges and universities operate some of the world's largest collections of computers and high-speed networks.

Taken altogether, higher education represents a great national resource with which to explore solutions and develop strategies for cybersecurity. It is a complex, technologically robust community that requires and achieves broad access to information and flexible, high-speed communications. The open, innovative values of higher education are, in the end, those of the nation. Their computers and networks represent, in many cases, the emerging systems of the future. Successful security implementations in higher education can serve as guideposts for the nation at large.

American higher education is a large collection of institutions and systems that vary widely in scope, size, mission, and technical capability, loosely organized through a variety of associations. Several of these associations, including EDUCAUSE and Internet2, focus directly on information technology (IT) at the campus level. Major national associations for higher education also participate in coalitions such as the Higher Education Information Technology Alliance (HEITA) to coordinate executive-level action on issues of IT policy.

The educational mission of most campuses now requires direct access to computing and the Internet for every student. Issues of student turnover, evolving technology, technical diversity, decentralized management, funding, and the sheer size of the populations involved present special challenges for cybersecurity in the "wired" as well as the "wireless" campus. The research mission in higher education is critical to national innovation but presents a set of unique security challenges. The complexity of the campus outreach mission can approximate that of e-Government initiatives.

Despite its diversity, the academic community shares basic values, such as intellectual freedom and a decentralized approach to management, that emphasize professional rights and responsibilities. These strongly held beliefs affect the types of cybersecurity measures that succeed on campus, and they must be taken into account in any successful strategy. But in the end, security is essential for the protection of the academic culture.

Critical issues for cybersecurity in higher education vary at two levels: among institutions and among departments in a single institution. No one-size-fits-all solution will work. Although many of the issues are shared with other sectors, a few of them are more critical in higher education.

EDUCAUSE organized an online survey of the community on the questions to be addressed in the National Strategy to Secure Cyberspace. The results have been tabulated and will be used to help define a strategy for moving forward. Similarities to and differences from other segments of the economy have emerged from the results and help to emphasize the importance of increased sharing of information and best practices.

National leaders of higher education have endorsed a five-part *Framework for Action* for cybersecurity and are organizing a series of four NSF-sponsored workshops that will involve the entire community in the development of a more coherent national strategy.

In summary, higher education plays a critical role in cybersecurity for the United States. It is now organized as a community to study and address this issue on a national scale, has the will and the endorsement of its top national leaders, and is well positioned to work with the federal government and other sectors on both traditional and innovative solutions.

Submitted by the staff of EDUCAUSE on behalf of the higher education community. For further information about this report or the EDUCAUSE/Internet2 Computer and Network Security Task Force, contact Rodney Petersen at 202.872.4200 or rpetersen@educause.edu

Introduction

The information and communication resources of the Internet, now considered a critical part of the national infrastructure, are indispensable to research and education. Ninety percent of all students and faculty access the Internet each day. Free and open exchange of information lies at the heart of the academic enterprise and is essential to both the education and research missions of America's colleges and universities.

A measured national response to the threat of terrorism must include steps to strengthen and protect the security of college and university networks and information resources. In addition, institutions of higher education have a responsibility to ensure that their computing and networking facilities not be used to launch attacks on critical infrastructure beyond the campus. As we respond to these new needs for cybersecurity, it is vital that we assess specific actions carefully and balance them with the fundamental commitment to freedom and openness that is at the very heart of our academic values.

The higher education sector represents a great national resource with which to explore solutions and develop strategies for cybersecurity in an open and free society. The values of higher education are, in the end, those of the nation. The computers and networks of higher education represent, in many cases, the emerging systems of the future. Successful security implementations in higher education can serve as guideposts for related developments in the nation at large.

The Commitment to Cybersecurity in Higher Education

Aspects of cybersecurity have long been of interest to individual campuses, systems, and consortia, illustrated by such phenomena as hiring security officers to track and fight incursions, hosting regional meetings for professional development and information sharing, and updating policies to reflect new levels and types of threats. The Massachusetts Institute of Technology, the University of Michigan, the University of Washington, Carnegie Mellon University, Indiana University, and others have pioneered security technologies, policies, and methodologies that are now widely deployed on a commercial basis.

The Consortium for Research and Education Networking (CREN) has organized the development and testing of a Public Key Infrastructure (PKI) Certificate Authority for higher education and is working with others such as Internet2, EDUCAUSE, and member campuses on the deployment of related policies and applications. EDUCAUSE is working with the Federal PKI Steering Committee and the National Institutes of Health to deploy a PKI "Bridge Certification Authority" for higher education that will interoperate with the existing Bridge Certification Authority of the federal government. These contributions have certainly made the overall situation better than it was before and have produced good results in specific, local circumstances.

More recently, the higher education sector has completed a number of significant, concrete steps to move forward with cybersecurity on a national basis. The locus of discussion and planning is in the EDUCAUSE/Internet2 Computer and Network Security Task Force, organized in summer 2000. In early 2002, the task force drafted a five-part *Framework for Action* that pledged to:

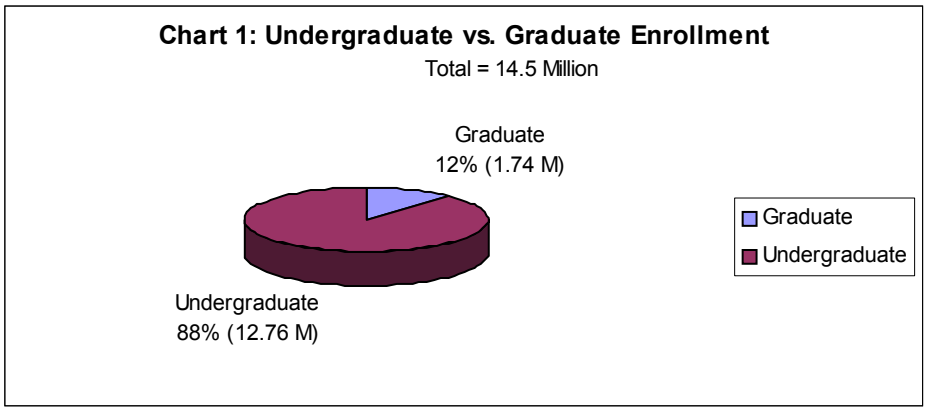
1. Make IT security a higher and more visible priority in higher education
2. Do a better job with existing security tools, including revision of institutional policies
3. Design, develop, and deploy improved security for future research and education networks
4. Raise the level of security collaboration among higher education, industry, and government
5. Integrate higher education work on security into the broader national effort to strengthen critical infrastructure

This *Framework for Action* was ratified by the American Council on Education and the remaining members of the Higher Education Information Technology Alliance (HEITA) in April 2002 and was presented to Richard Clarke, Special Advisor to the President for Cyberspace Security, when he addressed Networking 2002, an annual national policy meeting for campus information technology leaders. The task force now plans to coordinate four National Science Foundation-sponsored workshops to develop a more detailed strategy to improve cybersecurity across the sector. Included will be a collection of best practices organized by type of institution and guidelines for organizing for cybersecurity. Some of the challenges involved in this process can be illustrated by taking a closer look at the nature of the community of higher education in America.

Demographics of American Higher Education

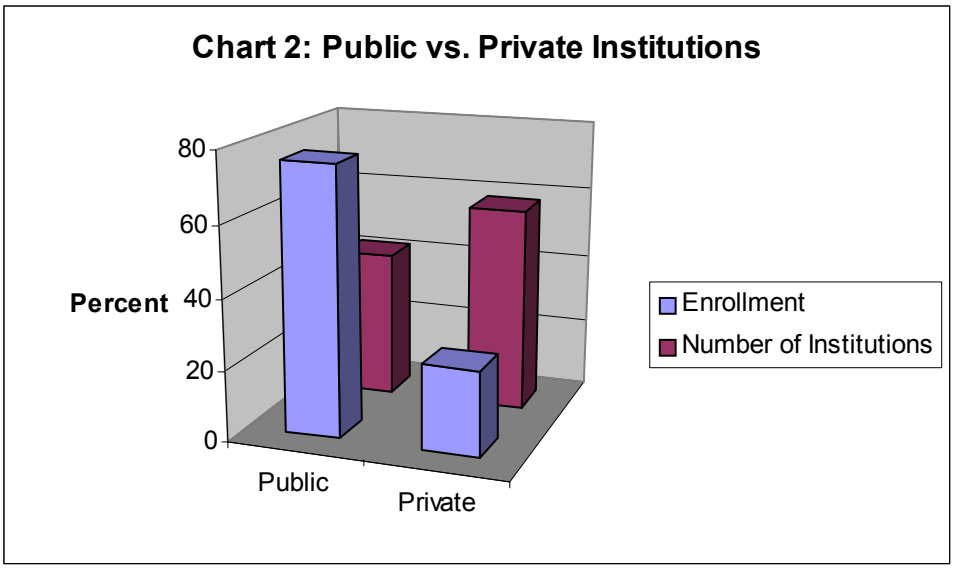
Higher education has emerged as a discrete sector of the United States economy. Its institutions share many characteristics and goals, yet vary tremendously in type, size, mission, resources, and complexity. Some elements of a strategy to secure cyberspace will be applicable to every institution while other elements might apply only to particular institutions. For optimal success, a strategy must be adaptable to the situation of each campus.

The United States higher education community comprises more than 11,000 post-secondary educational institutions. The strategies identified within this report are largely intended for the 4,048 accredited, degree-granting colleges within the American system of higher education. These institutions collectively serve 14.5 million students (both graduate and undergraduate – see chart 1), employ 3 million faculty and staff, and have combined budgets approaching $200 billion.



US Dept. of Ed. Digest of Educational Statistics 2000

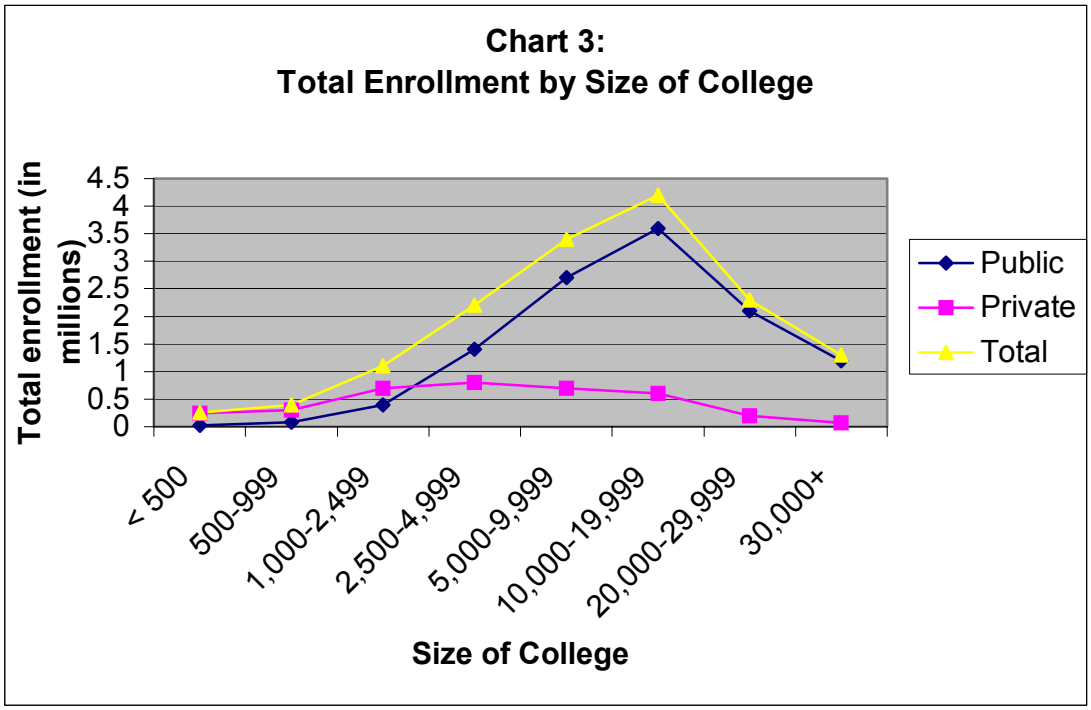
Seventy-six percent of all students are enrolled in a public college or university despite the fact that only 42 percent (or 1,681) of institutions are considered public (see chart 2). The public versus private distinction is significant for a number of reasons, including differences in governance structures, legal context, and funding models. Public colleges and universities rely considerably on funds from state governments and are often responsible for services to citizens of a specific geographic community. Many are considered agencies of state government and are subject to various regulatory and political considerations. Most states have established systems of higher education that link several institutions to each other, often with a collective governing board. Given the range of variation, no single model can describe public postsecondary institutions in the United States.



US Dept. of Ed. Digest of Educational Statistics 2000

Of the 4,048 institutions represented, more than 40% are two-year schools. While their enrollment numbers may be similar, these community-based colleges generally serve a student population whose needs vary from those in the traditional, residential four-year college setting. Their career orientation constitutes an economic entry point for much of this country's technical workforce, including preparation for careers in computer security.

The remaining 2,267 schools are four-year institutions that award bachelor's degrees. Over half of them award master's degrees, and 488 (or 20%) have doctoral programs. Enrollments at colleges and universities vary in size from fewer than 200 students to more than 40,000; the majority of schools have a student population of 10-20,000 (see chart 3). Institutional use of technology varies as well, from the small liberal arts college whose main enterprise computer is largely devoted to administrative and library services, to the large research university equipped with supercomputers and advanced networks, heavily involved in cutting-edge science and engineering.



US Dept. of Ed. Digest of Educational Statistics 2000

Of these 4,048 institutions, 140 participate in a significant level of funded research and development. The federal government invests an average of $16 billion dollars annually in university research programs—as much as $770 million in the case of Johns Hopkins University. All of these research programs involve the use of network technology at some advanced level, and many are directly involved in the development of the computing and network technologies of tomorrow.

Organization of American Higher Education

American higher education comprises a large number of institutions and systems of institutions with little hierarchical structure. Many are members, either directly or indirectly, of the American Council on Education (ACE) and are represented by their presidents in more specialized organizations such as the Association of American Universities (AAU), the National Association of State Universities and Land Grant Colleges (NASULGC), the American Association of State Colleges and Universities (AASCU), the National Association of Independent Colleges and Universities (NAICU), and the American Association of Community Colleges (AACC). A single institution may be a member of several of these associations.

Chief information officers, the top campus leadership of computing and networking, and many other IT professionals participate in EDUCAUSE, an association that addresses all aspects of computing and networking on campus. Many research institutions are also members of Internet2, which focuses on advanced networking for research and education. There are also numerous associations that support administrators and faculty based on special professional interests or academic disciplines and research foci, including computer security.

In recent years, a number of the major higher education associations have banded together to form the Higher Education Information Technology Alliance (HEITA) with the aim of developing a shared vision of IT policy issues in higher education. It recently endorsed the *Framework for Action* on cybersecurity, previously described. Members of HEITA include the following:

- American Association of Community Colleges
- American Association of State Colleges and Universities
- American Council on Education
- Association of American Universities
- Association of Research Libraries
- EDUCAUSE
- Internet2
- National Association of College and University Business Officers
- National Association of Independent Colleges and Universities
- National Association of State Universities and Land-Grant Colleges
- University Continuing Education Association

Cybersecurity and the Mission of Higher Education

The wide range of colleges and universities in the United States share all or most aspects of a three-part mission that sets broad requirements for access to networking and computing: *education, research, and outreach*.

Education

As might be inferred from the above demographics, the higher education sector comprises a wide variety of institutions with a range of specific missions, from focused professional schools to “multiversities” that rival cities in scope of activities and operational complexity. At the most basic level, all are concerned with teaching and learning.

The educational process is increasingly seen not as transmitting static knowledge from teacher to student but, rather, as a complex, interactive effort in which the learner engages ideas, applies principles and skills, and solves problems with guidance and encouragement from the teacher and in collaboration with other learners. This approach to education depends on easy and direct access to information in all its forms and on good support for communication and collaboration between students themselves, their teachers, and others around the world.

Active learner-centered education is essential for full participation as a citizen in an increasingly networked society and has become possible only recently through the development of the Internet, the Web, digital libraries, e-mail, threaded discussions, and related technologies. Access to these technologies and tools has become critical and is no longer considered a luxury. This is one reason why there has been such a major push to “wire the campus,” providing each student with direct access to computers and the Internet.

At the same time, campus demographics have shifted to include many more students with nontraditional backgrounds, including students outside the ages of 18 to 22 who live and work away from campus. These trends have stimulated major planning and investment in Internet-based solutions, causing many campuses to begin shifting much of their support operations and instructional resources to the network. The bottom line is that the core mission of teaching and learning has generated a nearly universal requirement for direct access to the Internet and other IT resources by every member of the campus community.

Of course, higher education plays a principal role in the training of security experts, both for employment in protecting the cyberinfrastructure of other sectors and for research in security methods and technologies for the future. The support and growth of this specialty will be critical for an effective national strategy for cybersecurity.

Research

Although relatively few institutions of higher education are engaged directly in funded research, the modern research university is recognized as the most successful approach to date for the development of new knowledge, methods, and technologies as well as the production of new scholars and skilled professionals. Basic research, housed primarily in institutions of higher education, seeds the applications and economies of the future. It has been of spectacular consequence for the areas of computing and networking during the past few decades.

In recent years, increasing numbers of disciplines have recognized that productive research requires direct access to very large computers on very fast networks. With the help of federal research agencies, higher education has stepped up to the challenge with such large-scale networking and computing projects as Partnerships for Advanced Computational Infrastructure, Internet2, and grid computing. Higher education now supports some of the world's largest collections of networked resources and maintains high-speed links to similar organizations around the world. In fact, it has been estimated that the research and education community accounts for approximately 15% of the total advertised addresses on the Internet.

Outreach

Many institutions of higher education today support an active program of outreach, that is, working with their neighboring communities to apply knowledge and skills available on campus. Outreach is also a two-way exchange that provides information, experience, and service in support of teaching and research. Key to successful outreach is the convenient flow of information between participants on campus and off. This segment of campus activity has embraced the Internet as a means to improve its effectiveness. In the future, high-quality online support of outreach activities will present the same kinds of opportunities and challenges as the e-Government initiatives.

Cybersecurity and the Values of Higher Education

Although institutions of higher education present a diversity of missions, there is widespread agreement on a few basic principles: academic and intellectual freedom, personal responsibility, diversity, and multiculturalism. These principles are critical for designing successful approaches to cybersecurity in higher education.

Academic freedom has a long, public history in higher education as a set of rights and responsibilities that enables inquiry, debate, and the pursuit of knowledge in new directions. This history is closely related to the library community's promotion of intellectual freedom and the constitutional guarantee of freedom of speech. Academic freedom is widely supported in America, not just as a right but as an essential requirement for the innovation and discovery that will drive our future capabilities as a nation.

Few institutions of higher education support a top-down management culture in which the organization chart determines control of daily affairs. Most colleges and universities function more as a decentralized collection of professional organizations. Many faculties (and increasingly students and staff) participate by democratic means in the overall governance of the institution. Individual faculty members defend their autonomy as essential for innovation and discovery. Expectations of academic integrity, codes of conduct, and institutional policies establish community standards to which students and faculty alike are held. Rigorous systems of due process, often administered by peers, are common in both public institutions (under constitutional mandates) and private institutions (usually as the result of contracts).

Students are typically the largest component of the campus community. Even though the core mission requires that all have convenient access to the campus network and the Internet, the student viewpoint on the use of technology may differ considerably from that of the faculty and staff. One of the unique challenges for a residential campus is recognizing that student use of the network may be as much for personal entertainment as for the academic or business purposes that are typical for faculty and staff.

Most members of the campus community are rigorously opposed to any unjustified restriction of their use of networks and computers. At one level, this is a technical argument. Entire new sectors of our information economy can be traced back to the unique campus environment that affords its members, from the president to the undergraduate, the unfettered opportunity to explore new ideas and designs using powerful network connections. A recent study by the National Research Council supports the conclusion that the open nature of the Internet and campus networks has been an important factor in the rapid and flexible development of innovative applications.

At another level, opposition to regulations and restrictions may be an implicit reflection of individual priorities. Research faculty and their graduate students, for example, are oftentimes intensely focused on “doing their experiment,” and not on computer system administration. Although insistent on protecting the intellectual property of their work, they may not see cybersecurity as a related issue until after the fact of an incursion. Since research funding and administration (including the operation of research computers) is largely decentralized to the faculty or the lab, many security problems have received inadequate attention in the past. This issue is now receiving considerable attention in the community.

All this is not to say that cybersecurity cannot be achieved for a college or university. Rather, successful solutions must work within the culture, appealing in meaningful ways to the goals of the community. One critical activity for each campus to consider is open discussion of the interplay of academic values and cybersecurity. In the end, cybersecurity is essential to the protection of academic values. Solutions that work in the environment of higher education will be important to the nation as a whole, since the same values of openness and innovation are widely shared throughout the nation.

Computer and Network Infrastructures in Higher Education

It goes without saying that plans to improve cybersecurity on a campus must take into account the types and arrangements of computer systems and networks involved and the human and other resources that can be applied to the solutions. These factors can vary widely between institutions. A single campus network may host systems as dissimilar as a supercomputer cluster involved in international research, a mainframe running payroll, and a student-owned laptop.

Enrollment also makes a difference. Solutions designed for a university with a student population of 30,000 would likely be out of reach for a small liberal arts college. Likewise, management problems that arise on a smaller campus can grow to enormous proportions at a school equipped with an abundance of high-speed computing power. The following are security issues that depend on an institution's size and available resources:

- How is the campus connected to the Internet? Smaller campuses may obtain their Internet connectivity from a single, commercial Internet service provider or from a regional academic network, which might also be responsible for basic security services and other kinds of technical support. Large research institutions, on the other hand, may have multiple Internet connections, both for redundancy and because of affiliations with Internet2 or other leading-edge network activities.

- *What degree of technical expertise resides within the institution?* To what extent can the campus evaluate and use a wide range of available solutions and customize off-the-shelf options? How much outside help is available?

- *What degree of central control can the campus impose?* On campuses where control of computers and networks is highly distributed, solutions will tend to focus more on borders and interconnections – places where central control can be imposed – and less on individual computers and local networks. The issue of central control also relates to campus policies and the campus judicial or disciplinary systems. On some campuses, a great deal may be accomplished simply by setting appropriate policies; on others, focusing on specific technological constraints will be more important.

The variety of technology within a single institution presents an additional security challenge. Issues that revolve around disparate systems include:

- *How can the campus network be segmented – perhaps physically, but most likely virtually – so that the various types of systems and networks can each receive its appropriate level of security?* With appropriate segmentation, for example, there is no reason that the institution's administrative systems cannot be as secure as those of conventional private sector corporations.

- *How do student-owned computers connect to the campus network?* At nonresidential colleges, student connections are typically made through modem pools or commercial Internet service providers. In residence halls, on the other hand, student-owned computers generally are connected directly to the same network infrastructure as administrative, research, and instructional systems. Student-owned computers can easily represent the largest number of computers making use of campus resources, but at the same time they are the most difficult to standardize or to control.

- *What types of special-purpose systems exist on the campus?* Medical systems, for example, may have life-and-death implications, as well as special legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA). Special security solutions will nearly always be required for such systems.

And finally, when considering the types of computer systems and networks to be secured, several issues cut across all of higher education:

- *Budgets are tight, and many of the benefits of increased security are often perceived to have little direct payback for the institution itself.*

- *Campuses are subject to the same security flaws in vendor products that affect the rest of the world.* Because of the diversity of computers and users, these flaws often impact higher education disproportionately.

- *Technology keeps changing, and new security issues are introduced with each new technology.* For example, the recent popularity of wireless connections carries a new concern about data (including password) exposure. Today's security solutions are likely to become quickly inadequate as handheld devices proliferate and as these devices merge with cellular telephones to become generic communication appliances.

Responses to Questions for the National Strategy

As part of its preparation for the *Framework for Action*, EDUCAUSE conducted an online survey of the higher education community based on the fifty-three "Questions to Be Addressed" of the White House's Critical Infrastructure Protection Board. Members of the higher education community were invited to address three questions that specifically concerned higher education at the EDUCAUSE Web site and were encouraged to read or respond to the full survey available elsewhere. The request was broadcast widely to members of EDUCAUSE, Internet2, and associations such as the Higher Education IT Alliance. Elements of this survey on the National Strategy will play an important role in implementing the *Framework for Action*.

Approximately one hundred answers were received and tabulated. One common thread throughout the survey results was the similarity between the operations of cyberinfrastructure in higher education and in other business or government organizations. It was often noted that the campus network includes nearly all the features of a broadband ISP for residence halls, a corporate information and transaction center for campus administrative systems, and a very decentralized collection of departmental and laboratory LANs for research and education. Therefore, a key action item would be to develop and document best-practice technologies, policies, and operations for cybersecurity in higher education with such major divisions in mind. This may include looking outside the academic community for solutions in similar systems.

Additional responses are summarized below by question:

- Preventing Attacks from Universities
- Preventing Attacks within Universities
- Organization and Coordination

Preventing Attacks from Universities

How can academic freedom of inquiry be maintained while preventing the large-scale computing power of universities from being hijacked for denial of service attacks and other malicious activity directed at other sites?

Of primary concern for all respondents was the need to maintain the balance between intellectual freedom, privacy, and security. Consistent with this view, the American Association of University Professors Statement on Academic Freedom in Electronic Communications (available at http://www.aaup.org/statements/SpchState/Statelec.htm) argues that reasonable measures of computer security which do not impede research generally do not inhibit academic freedom. Providing adequate security measures is a responsibility that helps ensure the continued right to privacy and freedom.

To achieve this balance, responses support a three-pronged approach: Measures must be taken at the *administrative level*, the *user level*, and the *technical level*. At the administrative level, staff must develop and enforce a technology policy that conforms to their particular environment. The policy should be based on metrics, have an established baseline, and promote the collection and use of data to analyze security problems relative to other sources.

A user education program as well as consistent enforcement measures should be established to focus on apprehending security violators, not just changing the system or network used for the attack. Users should be made aware of their role in maintaining a secure network, as well as proper network etiquette and the consequences of misuse.

At the technical level, systems should be checked against the SANS/FBI Top 20 list (see http://www.sans.org/top20.htm) and similar sources of known vulnerabilities on a regular schedule. Operating system software should be kept current with the latest known patches and vendor security solutions. Suggested security technology includes selectively placed firewalls, intrusion detection systems, antivirus software, secure file

transfer protocol (ftp), e-mail virus filtering, personal firewall software, configuration and security protocols, strong passwords, vulnerability scanning, public key infrastructure, and digital signatures. Apart from avoiding vulnerabilities, higher education should actively participate in research, development, and testing of new technologies to detect and mitigate denial of service and related attacks on others.

Questions for further study:

How can the great complexity of existing custom solutions be parsed into a small number of models that can be adapted to fit most colleges and universities? How can we identify a manageable set of model policies, practices, and technologies on an ongoing basis? How can we share this information across the sector? How can we best achieve executive support at the institutional level? How can higher education best coordinate its on-campus security operations with others who may be the subject of attacks?

Preventing Attacks within Universities

What functions and applications supported by a university system require high levels of IT security (e.g. medical records, student records, research trials, patents) and how is this best achieved within the context of an academic setting?

The administrative role of establishing a security architecture that identifies the level of protection needed and incorporates appropriate policies and technologies was a theme throughout the responses to this question. Every campus runs at least three distinct types of networks (for research, for business purposes, and as an Internet Service Provider). Protecting the electronic resources of libraries may be very different from securing a business system that processes personal information and financial transactions. The regulatory context already includes requirements related to HIPAA, the Family Educational Rights and Privacy Act (FERPA), and various state laws and regulations. Additional need for regulation at the federal or state level is minimal.

Questions for further discussion:

Many of the issues that arise in preventing attacks from universities are also encountered in preventing attacks within universities. How can we best differentiate our technologies, policies, and operations to provide the right degree of protection for the different types of campus information and resources? What concrete steps can we take to improve the security of critical and private information that is collected and maintained in research systems? What solutions work best in the culture of distributed management and authority? How can universities best address these problems at the institutional level?

Organization and Coordination

How can universities best organize to address the IT security questions they face in common? Should best practices or standards be agreed to on a national level? Should there be a mechanism for information sharing on threats and vulnerabilities among university CIOs and systems administrators?

The survey results indicate the need for improved communications between all entities involved in network security as in the recent report from the Computer Science and Telecommunications Board that recommends creating a central clearinghouse for information regarding infrastructure security. This includes reaching beyond the state level to industry and the federal government for information and resources. Many communication mechanisms already exist (e.g. SANS, UNISOG, CERT, InfraGard, etc.); however, it would be beneficial to streamline and strengthen communications within the higher education sector, providing a more focused source of information for the community. EDUCAUSE is seen as an appropriate entity to help organize and coordinate some of these efforts. In addition, colleges and universities should designate a chief security officer to garner resources, oversee operations at the local level, and act as the conduit for participation in the national dialogue. Again, government oversight, except for information exchange, should be minimal.

Questions for further study:

What is the most effective way to share information on best practices across the sector? Among sectors? What is best for ongoing critical alerts? Is there a single answer for higher education, or is it best to organize according to institutional types? How can research and education institutions contribute to the development and testing of new solutions on a national scale?

Framework for Action for Cybersecurity

The *Framework for Action* will serve as the basis for coordinating a wide variety of activities—at the campus level as well as at the national level—which are needed to strengthen the security of higher education information technology systems and resources. The *Framework* has been formally ratified by the leadership of higher education through the American Council on Education and the Higher Education IT Alliance. The five-part action plan follows.

1. Make IT security a higher and more visible priority in higher education.

Security for campus computers and networks, especially physical security, is not a new responsibility for higher education managers. But the events of September 11, 2001, highlighted vulnerabilities in these systems that had not been dealt with adequately in the past. Many campuses, in the face of numerous competing demands for technical and management resources, have failed to adjust to the increasing dependence of their research and educational mission on secure systems. A major part of an improved security posture, therefore, will be increased management attention to campus IT security programs, including the top executive leadership of the institutions.

2. Do a better job with existing security tools, including revision of institutional policies.

Security touches nearly every aspect of computers, networks, and their use. It is common knowledge that existing systems are vulnerable, amply demonstrated by the extent of damage caused by recent network worm and denial of service attacks. Although the success of many attacks can be attributed to deficiencies in computer operating systems and applications software, in many instances, breaches of systems have occurred because users neglected even the most rudimentary protections already offered by the makers of their systems. Therefore, a first order of business is for everyone with responsibility for computers, information servers, network components, and other parts of campus IT infrastructure to bring their systems up to the most current level of security supported by vendors.

Additionally, existing policy statements covering individual, managerial, and institutional responsibilities for security are in many instances out of date and do not reflect current circumstances. These also need updating to ensure that a set of common expectations about security responsibilities is established and followed.

3. Design, develop, and deploy improved security for future research and education networks.

One of the important challenges in academic networking is to ensure a continuing flow of performance improvements and other forms of innovation so that the community has access to the very best information technology tools to support research and teaching goals. In some respects, the improvement of security, in both current and future networks, competes with performance goals. This is especially true when performance and security are not part of the initial network design process, as has commonly been the case up to the present time.

A significant effort must be undertaken to develop high performance networks that have security built into them. Architectural tradeoffs must be examined, experiments conducted, and the results widely disseminated to network developers and manufacturers.

4. Raise the level of security collaboration between higher education, industry, and government.

The design, development, and deployment of networks, especially the Internet, have historically been a joint effort among government research agencies, university researchers, and computer industry firms. A coordinated response to the need for significant improvements in network security requires the continuation and strengthening of collaboration in research, development, and technology transfer. New federal funding for security research must flow to the research and development community, and aggressive efforts must be made to ensure early deployment of successful research results.

5. Integrate higher education work on security into the broader national effort to strengthen critical infrastructure.

In the aftermath of September 11, 2001, federal, state, and local governments are making rapid changes in their security arrangements in order to respond to potential terrorist attacks, especially on critical infrastructure. Higher education networks and IT resources are an important part of the nation's infrastructure, and the response within higher education must be coordinated effectively with agencies having responsibility for national security and public safety.

Next Steps

The *Framework for Action* identifies the overarching action steps that are needed to improve information technology security in higher education. Additionally, the initial responses to the questions summarized above, including questions identified for further study, will be further examined and refined in a series of activities planned at the campus and the national levels.

Developing a Strategy for Higher Education through NSF Workshops

In order to effect significant change and ensure the broadest and highest possible level of participation, the higher education community is planning a number of complementary efforts over the next several months. Central to the goals of increasing awareness and developing a concrete security strategy for higher education is a series of four National Science Foundation-funded workshops during the second half of this year, bringing together key stakeholders in the higher education community.

The first meeting will establish principles for a higher education security strategy. Two of the greatest challenges in establishing a strategy for securing cyberspace are determining how much security is enough and shaping the strategy in such a way that it upholds the fundamental values and mission of higher education. While improved security is expected to change existing cultural norms within colleges and universities, it will be important to any strategy's success that future direction be bound by universally understood principles and a framework that supports higher education's mission of teaching and learning, research and discovery, as well as outreach and service. A one-day working conference of invited leaders in the higher education community will be convened to develop principles that articulate the common values and mission of higher education that will serve as a benchmark for subsequent discussions and plans.

The next meeting will invite a small number of higher education IT security and policy professionals to identify problems, issues, and opportunities for improving computer and network security. EDUCAUSE will design and facilitate this two-day working conference, focusing on problem identification, technical solutions, and policy requirements for providing a secure computing environment. The results will be shared with participants in subsequent events, including the user communities meeting and the summit described below.

The third meeting will include members of the research and user communities to discuss the growing external pressure and internal concern about creating secure computing environments to support faculty and student research activities. The issue is especially important when researchers collect or have access to sensitive data, connect to remote computer systems, and rely upon others for system operation or computer support. There is also an emerging need to identify issues and establish appropriate policies and plans that will be applicable across research institutions. The results will be shared with summit participants and will be considered in proposed solutions.

Finally, broad executive-level education and support are needed to develop an effective, coordinated strategy for higher education computer and network security. EDUCAUSE will design and facilitate a summit of higher education administrators and appropriate experts to raise awareness and create an opportunity for shared responsibility. The meeting will include members of the EDUCAUSE/Internet2 Computer and Network Security Task Force and invited attendees from the higher education community, including presidents, vice presidents, chief information officers, librarians, risk managers, internal auditors, legal counsel, registrars, business and finance officers, and other key administrators. Key higher education associations will also be represented.

Commissioned Works and Research Projects

The EDUCAUSE/Internet2 Computer and Network Security Task Force will also commission works on important topics such as a primer on legal issues and risk management, analysis of IT security plans and policies, description of models for IT security organizations, models and templates for conducting computer security risk analysis, and the development of security incident case studies. Although there is moral support throughout the higher education community for the development of best practices, the security professionals dedicated to resolving the current crisis have little time to study and document problems and solutions. The commissioned research projects culminating in papers, reports, and case studies are critical to both problem identification and support of the extensive professional development needs of the higher education community. The results will be shared with summit participants and will be refined for later publication and broader dissemination.

In an effort to facilitate broad engagement, the task force will continue to conduct outreach for the higher education community. Developing a strategy for higher education will be an ongoing process requiring extensive discussion, refinement, and regular updates.

Identifying Best Practices and Sharing Common Solutions

Higher education has a tradition of sharing information, and this tradition can be of great benefit to enhancing computer and network security on campuses. Organizations such as EDUCAUSE, the Common Solutions Group, Internet2, the Higher Education IT Alliance, and the American Council on Education can help identify and disseminate best practices and common solutions. Security staff within higher education also participate in security-related organizations well known for information sharing such as CERT, CIAC, SANS, and InfraGard, both as contributors and consumers. EDUCAUSE and

others in the community can play a more active role in sharing emergency alerts, such as the recent warnings on incidents of surreptitious key logging.

Because of the diversity of higher education's needs, there is no single set of best practices that will apply to all campuses. Rather, the goal is to provide a range of solutions proven to work well in particular environments. Several exemplars provide good starting points. The Institute for Computer Policy and Law, sponsored by EDUCAUSE and Cornell University, maintains a database of policies from several hundred campuses, including policies covering all aspects of technology security.

In one way or another, all institutions must address these goals and requirements:

- *Detect and prevent attacks against campus systems originating from off-campus.* New risks of misuse of networked computer systems have emerged in addition to the traditional threats of theft or misuse of institutional data. Hackers want to control campus computers to use them as launching points for further attacks or as repositories for contraband. For this reason, successful attacks are often invisible to the owners of the subverted systems. Higher education is uniquely situated to be the target of such attacks, making information sharing within the community particularly important.

- *Detect and prevent attacks originating from the campus aimed at off-campus systems.* Even when such attacks are actually controlled by hackers who have taken over campus computers, it is up to the campus to solve the problem. The looming possibility of widely distributed denial of service attacks makes a solution increasingly important.

- *Secure vital campus systems and data against on- and off-campus threats.* This goal can be translated beyond higher education to all sectors of the nation's cyberspace. Information sharing and best practices here will likely parallel solutions developed by industry and government.

Conclusion

The higher education sector plays an important role in the cybersecurity of America. Through its core mission of teaching and learning, it is the main source of our future leaders, innovators, and technical workforce. Through research, it is the basic source of much of our new knowledge and subsequent technologies. And finally, as institutions, colleges and universities operate some of the world's largest collections of computers and high-speed networks.

Higher education is now organizing to study and address cybersecurity issues on a national scale. It has the will and the endorsement of top national leaders of the community and is well positioned to work with the federal government and other sectors on both traditional and innovative solutions.

Taken altogether, higher education represents a great national resource with which to explore solutions and develop strategies for cybersecurity. It is a complex, technologically robust community that requires broad access to information and flexible, high-speed communications. The open, innovative values of higher education are, in the end, those of the nation. The computers and networks of higher education represent, in many cases, the emerging systems of the future. As a consequence, successful security implementations in higher education can serve as guideposts for related developments in cybersecurity for the nation at large.