

INFORMATION TECHNOLOGY CRITICAL INFRASTRUCTURE IN HIGHER EDUCATION

A Framework for Action

Introduction

The events of September 11 have presented Americans with many challenges in accommodating their personal and work lives to a changed world in which the unthinkable is now potentially a daily reality. The nation's colleges and universities and their faculties, students and staff have a number of responsibilities in responding to new threats to long established patterns of research and scholarship. Foremost among these is the need to understand the root causes of terrorism and to bring the resources of the academic world to bear on both national policy and the personal responses of individuals in preventing a repetition of last year's catastrophe and in laying a foundation for a saner world in the future.

The information and communication resources of the Internet, now grown to become a critical part of the national infrastructure, are equally indispensable to research and education. The free and open exchange of information lies at the heart of the academic enterprise, essential to both the education and research missions of America's colleges and universities. A measured response to terrorism and terrorists must include steps to strengthen and protect the security of college and university Internet links, as well as those campus information technology resources which are essential to scholarship and vulnerable to attack. 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 network infrastructure beyond the campus, as has occurred in the past. As we respond to these new needs for security in our infrastructure, it is vital that we assess and balance specific security actions against the fundamental commitment to freedom and openness that is at the very heart of our academic values.

No action statement by itself will secure an open and accessible system of information technology resources for higher education. Given the ubiquity of the Internet in academia and the operational complexity of its workings, improvements in information technology security will require significant resources - tens of millions of dollars across several thousands of institutions. Some of the necessary work can be done with one time funding allocations, but a significant increase in existing or new security budgets will be required to sustain the increased levels of protection that are needed to address changed circumstances. Responding to new budget increases for information technology security in a time of constrained finances for colleges and universities will be a special challenge for academic leaders, their trustees and their funding sponsors at state and federal levels and within the private sector.

This document has been prepared by a security working group composed of experts from the ranks of the two major information technology management organizations in higher education - EDUCAUSE and UCAID (Internet2) - among whose joint membership are more than 1500 colleges and universities. It has been endorsed by a number of higher education membership associations representing both leadership and professional backgrounds and experience.

Supporting Organizations

In addition to Internet2 and EDUCAUSE, leading national higher education organizations have endorsed this framework to improve information technology security in higher education:

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

Background

The overall goal of improved information technology security in higher education is to create an academic Internet environment in which no combination of deliberate attacks, personal negligence or accidental oversights results in loss or damage to computers, their files and databases, or to networks themselves.

There are few absolutes in security work and the achievement of improvements will not always be apparent externally, since the result of good security is that failures are avoided. The steps proposed in this action statement and described in the following paragraphs are intended to provide an initial response to a new level of threat and a guide to creating an environment in which both users and providers of information and communications resources for the academic community can have confidence that the tools and systems on which their work depends will continue to be available to them.

The number and complexity of computers and associated network facilities across thousands of college and university campuses with millions of users requires that a comprehensive approach be adopted in which managerial, technical and operational responsibilities are clearly drawn and specific improvement actions are tailored to local needs. The plan described below includes five elements covering the major categories of effort that are required to achieve a measurable improvement in security.

Action Statement

The purpose of the security action plan numbered elements is to serve as the basis for coordination of 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.

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 have highlighted a vulnerability in these systems that has 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 information technology security programs.

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

Security touches nearly every part of computers and networks and their use. It is common knowledge, amply demonstrated by the extent of damage caused by recent network worm and denial of service attacks, that existing systems are vulnerable. Although the success of many attacks is attributable to deficiencies in computer operating system and applications software, it has also been shown that, 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 information technology infrastructure to bring their systems up to the mostly current available level of security supported by vendors of these systems.

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 among 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 security improvements in networks requires a continuation and a strengthening of that tradition of collaboration in research, development and technology transfer. New federal funding for security research must flow to the R&D 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, 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 information technology resources are an important part of the nation's infrastructure and the response within higher education must be effectively coordinated with agencies having responsibility for national security and public safety.