

Planning for Improved Security

College and university information technology staff and functional offices are clamoring for the development of an institutional “information security policy.” A helpful starting place would be a statement of strategic direction that identifies improvement of technology security as a priority and assigns appropriate authority to develop and implement a program. This approach is consistent with general policy processes, since policies should be based on strategies or plans established or endorsed by institutional decision-makers.

A technology security program must be designed to support the purposes for which the academic enterprise exists—teaching and learning, research and discovery, and outreach and service. It is easy to sometimes view security as the end-goal instead of as one activity among many others. An IT security program must maximize confidentiality, integrity, and availability of information and technology resources and must be approached as being an enabler of institutional processes.

Environmental Scan

A typical exercise for beginning any strategic planning process is to scan the environment and document the present state of affairs. At an NSF-funded workshop organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force in the fall of 2002, participants made observations about higher education technology and data environments and categorized them according to technology environment, leadership environment, and academic culture. Though

not considered at the workshop, the role of higher education in homeland security could be viewed as a fourth environment.

Technology environment. There is tremendous diversity in the type and quality of hardware and software utilized across an institution, ranging from outdated to state-of-the-art. The variety of equipment ownership—from student-owned computers to federally funded supercomputers—is also a complicating factor. The student population is transient and comes to campus with no real appreciation of security issues. Vendor products typically contain numerous and unnecessary security problems. The professional IT staff are often distributed and autonomous and lack accountability; good technicians are overworked and underpaid; many IT organizations and departments employ students with little or no systems management or security-specific training. Finally, the increased demands for distributed computing, distance learning, and advanced networking capabilities create unique security challenges.

Leadership environment. Higher education leadership tends to be reactive rather than proactive. The apparent lack of ownership of information technology security as an institution-wide concern results in the assumption that security is “someone else’s” problem. In many institutions, there is often a lack of strong centralized security leadership with the authority to mandate change and enforce policy across all campus constituencies. There is a lack of clearly defined goals based on assessment of risks and a lack of metrics with which to monitor compliance. Finally, there is an absence of policy general enough to allow for evolutionary change

and of associated standards that are practical, enforceable, and detailed enough to provide for a regular system of audit.

Academic culture. Some segments of the higher education community continue to believe that security and academic freedom are antithetical. Academic environments are characterized as communities of tolerance and experimentation, where anonymity is highly valued. IT staff often feel that tenured faculty value autonomy and privacy to a fault and are resistant to any new demand on their time or to constraints on institutional resources. Proactive security measures may be viewed as too “bureaucratic” by faculty, deans, researchers, and others in the academic arena.

Homeland security. According to network routing tables, higher education holds more than 15 percent of the Internet network addresses. Clearly, higher education must be a major player in ensuring that this portion of the national cyberinfrastructure is protected from logical and physical attacks. Campus networks and systems can be used—and have been used, in recent years—to launch attacks on commercial operations. More recently, several U.S. university networks were used to amplify attacks on the root name servers. Higher education must work to minimize the opportunity for terrorists and criminals to use campus networks and systems to further their nefarious activities.

Alternative Planning Approaches

Planning for IT security can be the result of a grassroots effort within the central IT organization, it can be an element of an IT strategic plan, or it can be integrated

into an institution-wide strategic planning effort. Whatever form it takes, developing a business case for investments in technology security is increasingly essential, especially given recent fiscal crises and competition for resources. There is not one “right” approach for crafting a successful IT security strategy. Each institution must evaluate its own unique interests, resources, and political climate.

Prairie dog approach. Unfortunately, increased attention to IT security is often stimulated by a major security incident—an event that causes heads to “pop up” all over campus. Such an event will clearly demonstrate shortcomings and vulnerabilities, and the resulting investigation and response to questions from the campus and the media can actually result in the creation of at least the outline of a security program.

External pressures. Yet another impetus for the creation of a security plan is governmental regulations and pressure. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Gramm-Leach-Bliley Act of 1999, for example, caused many colleges and universities to create or consolidate security, risk-assessment, and training programs and to assign responsibility for these programs.

University of California, Berkeley. At the University of California, Berkeley, a Security Working Group of the Information Technology Architecture Task Force (ITATF) was formed to address concerns presented by the ubiquitous use of computers and networks. The group’s report, issued in May 1998 (http://socrates.berkeley.edu:2001/security/itatf_swg_report.html), identified specific risks and recommended campus-wide security policies and planning, more centralized staffing for security measures, and centralized security training, among other items. The initial proposal was rejected due to budget limitations, but a more modest request that allocated a portion of the existing IT budget to the proposal was approved. A campus-wide security committee continues to meet regularly to help develop policies and procedures. An example of these efforts is the “Campus Information Technology Security Policy” (<http://socrates.berkeley.edu:2002/IT.sec.policy.html>).

University of Maryland. The first CIO for the University of Maryland (UM) arrived in 1998 and established a number of working groups to assess services and make recommendations about organizational structure. Noticeably absent from the organization at that time were any services or staff devoted to information security. Therefore, a Security Working Group was established to assess the current state of network and computer security at the university and to

provide recommendations for improvement.

The group benefited from the efforts of UC-Berkeley and of other peer institutions. As a result, UM has established the position of University IT Security Officer, has integrated information security items into both the University Strategic Plan and the IT Strategic Plan, and continues to pursue the recommendations first identified by the working group’s report (<http://www.oit.umd.edu/pp/docs/security>).

Indiana University. The IT strategic plan for Indiana University (IU) was published in May 1998 and continues to provide an aggressive and bold vision for how IT is developed and deployed at IU (<http://www.indiana.edu/~ovpit/strategic>). Specific to IT security, the plan states that security and privacy are important issues for IU to address in achieving a position of IT leadership. The plan identifies security of information and IT as university-wide concerns that require a university-wide response, including institutional vision and commitment, clear and forceful policies, appropriate plans and procedures, and ongoing programs of education and awareness. The CIO is encouraged to take a continuing, active role in leading this

university-wide initiative, and the president and leadership at the highest levels of the institution are encouraged to become engaged in these efforts. An action item was specifically associated with these statements in the plan, and as a result, significant funds were dedicated to various measures designed to improve the security of IT resources. Giving security a prominent place in a well-prepared and widely publicized plan has been instrumental in getting related issues recognized, discussed, and ultimately addressed at the highest levels within IU.

Conclusion

Significant progress has been made in improving the security of higher education information technology as a result of efforts of the EDUCAUSE/Internet2 Computer and Network Security Task Force, higher education-sponsored conferences, campus security days, increased interaction between campus technologists and security officers, and steps taken by other associations (e.g., ACUTA, NACUBO, NACUA, ACE) to encourage the discussion of security issues within their constituencies. Higher education will soon be able to shrug off the perception that the academic community is the bane of technology security. Even now, insecure home Internet connections are quickly replacing campus systems as the medium for many illegal online activities. Institutions are also revisiting the deployment of technologies previously discounted as being infeasible in diverse networks—technologies such as formal border firewall appliances, scanning services, and robust intrusion-detection systems. For higher education, the key factor for success in the security effort will be the ongoing development and refinement of effective security strategies and plans.

Mark Bruhn is Chief IT Security and Policy Officer for Indiana University and Associate Director of the IU Center for Applied Cybersecurity Research. Rodney Petersen is Project Coordinator for the Security Task Force and Policy Analyst at EDUCAUSE.

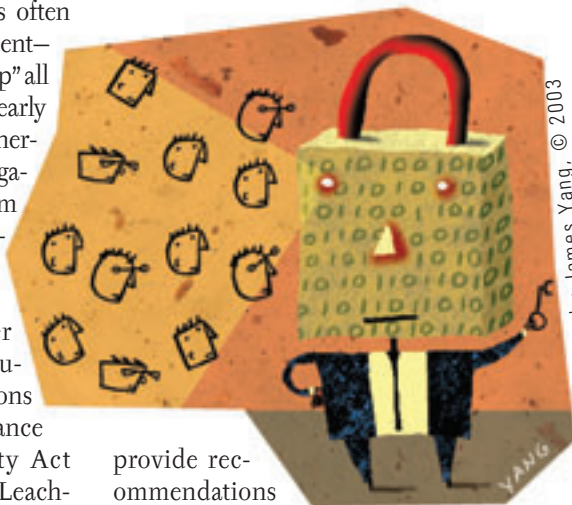


Illustration by James Yang. © 2003