

# Roadmap

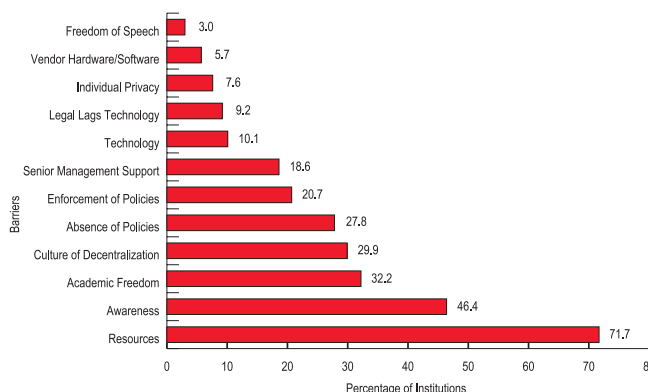
TOOLS FOR NAVIGATING COMPLEX DECISIONS

## Information Technology Security: Governance, Strategy, and Practice in Higher Education

By Robert B. Kvavik, Senior Fellow, EDUCAUSE Center for Applied Research, and Associate Provost, University of Minnesota

### KEY FINDINGS

- ▶ By far the most common barrier to IT security is resources (72 percent), followed by awareness (46 percent) and cultural factors—academic freedom (32 percent) and culture of decentralization (30 percent). Surprisingly, external factors such as laws and their timely implementation and clarification, technology, software, and hardware scored much lower.
- ▶ While deploying technology is necessary to achieve effective IT security, institutions must place equal if not greater weight on the “soft” aspects of security, including ongoing user awareness; creation of effective, understandable, and enforceable IT security policies; and effective communications.
- ▶ Involvement of the institution’s senior leadership with IT security is important to the security program’s success. It is difficult to create comprehensive programs and enforce IT security policies without senior academic and business officers’ involvement and support.
- ▶ The use of established technologies, such as firewalls and SSL, will be pervasive within several years. Use of newer tools, like enterprise directories and intrusion detection, appears to be growing rapidly. Emerging technologies, like electronic signatures and Shibboleth, are being adopted at a slower pace.



For well over four decades, providing secure information technology (IT) services to their constituents has been a top priority for college and university administrators. Institutions have invested money and human resources to protect their information assets and those of faculty and students. With no end in sight to security threats and breaches, institutional efforts are growing. For example, the EDUCAUSE Center for Applied Research (ECAR) study *Information Technology Security: Governance, Strategy, and Practice in Higher Education* reports that 20 percent of institutions now have a full-time security manager; half employ a full-time IT security staff.

However, rapidly increasing bandwidth demands, the evolution of distributed computing architectures (and governance), and an incredible rise in computer crimes continue to place increasing stresses on higher education’s computing infrastructures. Even institutions famous for their IT security investments and policies are at risk and have suffered newsworthy break-ins, resulting in the theft of student Social Security numbers and other confidential information. Colleges and universities have also been the launch pads for numerous newsworthy virus and denial-of-service attacks in recent years, creating high public-relations, financial, and regulatory exposure for higher education as a whole.

Nonetheless, the current state of colleges and universities with respect to IT security is largely anecdotal. We have little quantitative information on how distributed computing, distance learning, and mobile and wireless capabilities affect security. Leadership is

*This ECAR Roadmap synthesizes the responses of 435 senior college and university administrators, the majority of whom were CIOs and other IT leaders at higher education institutions, from an April 2003 survey as reported in Information Technology Security: Governance, Strategy, and Practice in Higher Education by Robert B. Kvavik and John Voloudakis. To order the full study and learn about subscribing to ECAR, visit the ECAR Web site at <http://www.educause.edu/ecar/> or contact us at [ecar@educause.edu](mailto:ecar@educause.edu).*

## **“Soft” or Nontechnical Checklist to Promote IT Security**

- ▶ IT security policies and plans to set the framework
- ▶ A dedicated IT security organization to promote professionalism and drive programs
- ▶ Formal awareness programs to educate staff on safe IT security practices
- ▶ Active leadership to promote security-conscious culture
- ▶ Adequate funding to facilitate implementation of effective security strategy

characterized as reactive rather than proactive, with a lack of clearly defined goals. Similarly, in academic environments the goals of security, academic freedom, and intellectual freedom are typically seen as antithetical. The ECAR study *Information Technology Security: Governance, Strategy, and Practice in Higher Education* provides a fact-based and national perspective of higher education’s security environment that can lead to the improvement of institutions’ cybersecurity. It establishes a security baseline for higher education and identifies what security policies, products, and procedures are currently in place.

### **“Soft” IT Security Strategies**

Interestingly, IT security is sometimes viewed as an issue falling mainly in the domain of institutional IT organizations, but *Information Technology Security: Governance, Strategy, and Practice in Higher Education* finds that while using technology is necessary to achieve effective IT security, the human—or “soft”—side often needs greater attention and frequently provides a greater sense of IT security. One component of the study’s research looks at a number of factors that could impact the sense of security felt by the respondents and analyzed those factors against five survey questions to assess respondents’ opinions on the success of their IT security programs (Likert scale ranging from 1 = strongly agree, 2 = agree, 3 = neutral, 4 = disagree, and 5 = strongly disagree):

- ▶ How would you characterize the success of your program?
- ▶ Has your institution gone beyond federal and state government IT security requirements?
- ▶ Are data, networks, and applications that are your responsibility secure?
- ▶ Have you developed metrics to determine the effectiveness of IT security activities?
- ▶ Is your institution more secure today than it was two years ago?

The study reveals the importance of several human and cultural factors to promote institutional IT security as outlined in ECAR’s checklist.

### **Policies and Plans Set the IT Security Framework**

Policies and plans enable IT organizations and institutions to map out a universal IT security strategy, providing an overarching framework while attending to day-to-day security issues. Just over half of the institutions surveyed (54 percent) indicated that they have formal institutional policies covering IT security. Comprehensive IT security plans are in place at 13 percent of responding institutions; another 78 percent reported that they either have a partial plan in place or are currently developing a plan. The study shows that institutions with IT security policies in place characterize their IT security programs as more successful and feel more secure today. Institutions with policies agreed more strongly (2.11) that their IT security programs were more successful than those without (2.55). The same is true when security is part of an IT plan and risk assessments have been completed. Security metrics are more likely to have been developed at institutions with IT plans and that conduct regular audits.

### **A Dedicated Staff Implements IT Security Programs and Policies Effectively**

When comparing the perceived success of IT security programs at institutions with a dedicated IT security staff, with a single staff member, or with a distributed staff, the mean response shows that institutions with a dedicated staff agree more strongly that not only is their IT security program successful (2.00) but also that the institutions have gone beyond federal and state governments recommendations for IT security (2.98). We attribute this to the activities undertaken and completed by a dedicated security staff, which has the time to see that various IT security tasks are completed. Existence of a dedicated staff (which was found to be more prevalent in larger institutions) is often accompanied by a high level of professionalism, which then drives what kinds of practices and procedures are in place and what technology is deployed. The number of staff employed was less significant than having a dedicated staff. The experience of the staff also seemed to make a difference. Institutions with individuals with more than three years’ experience felt they were doing better than institutions whose staff had three years’ or less experience.

## METHODOLOGY

- ▶ A literature review—to identify and clarify the major elements of the study and create a working set of hypotheses to be tested
- ▶ Consultation with a small and select group of IT security leaders in higher education—to identify and validate the most interesting research questions and hypotheses that would frame the quantitative survey instrument
- ▶ A quantitative survey of 435 higher education institutions
- ▶ Qualitative telephone interviews of 42 technology executives, managers, and faculty at 18 institutions

### Formal IT Awareness Programs Educate Users about IT Security “Do’s” and “Don’ts”

Fifty-two percent of the institutions in ECAR’s survey agreed or strongly agreed that IT security problems inadvertently caused by authorized users are a significant concern. Despite this perception, nearly 66 percent of institutions reported having no formal awareness programs in place for students, faculty, or staff. Awareness programs and security, however, are closely aligned. Institutions with IT security awareness programs for staff felt their IT security programs were more successful (2.00) than those without any programs (2.58).

### Active Leadership Promotes IT Security Conscious Culture

When presidents and provosts are active in developing IT security policy, it sets a tone about the importance of policy adherence and fosters a more security-conscious culture. At institutions where the president is involved, for example, the mean score for success is 3.18 versus 4.50 where senior leadership is uninvolved. Indeed, when security consciousness exists, constituents may begin to consider IT security as well as functionality when installing new systems or incorporating new business practices. For example, a majority of survey respondents (55 percent) indicated that business requirements take precedence over IT security when there is a conflict between the two. However, at those institutions where it was believed that security takes precedence, twice as many respondents indicated that their security programs are successful and that they feel more secure than they did two years ago.

### Money Matters When Developing IT Security Strategy

Absence of resources was by far the largest barrier to IT security for our respondents: almost three-quarters of survey respondents identified this as an obstacle. Fifty percent of the institutions reported that the budget for security represented 1 to 5 percent of the total central IT budget. As the percentage of the central IT budget spent on security rises, however, so do the assessment of the success of those IT security programs

and the perception of being more secure today than two years ago. Clearly, the more you spend, the better you feel! Similarly, if you believe the institution is providing necessary resources, the higher you rate the success of your IT security program and your current sense of IT security. The data also show that institutions that reported a higher percentage of the IT budget being spent on security—and where resources are sufficient—have purchased more technology and invested more in awareness programs.

### IT Security Technology and Practices

While “soft” elements contribute to IT security success, clearly an effective technical infrastructure and practices represent the first line of defense. Strategies used most often include limiting protocols allowed through the firewall or router (76 percent), restricting or limiting access to servers and applications (72 percent), and timing-out access to applications after an idle period (68 percent). Seldom used were installation of a directory inventory system to watch for undesired program changes (13 percent) and use of security devices for personal authentication (12 percent). *Information Technology Security: Governance, Strategy, and Practice in Higher Education* notes the adoption of the following IT security technologies and practices.

#### Firewalls

Firewalls are a key technology in higher education. Of all technologies employed by survey respondents, firewalls were the most commonly used (87 percent), and another 10 percent are currently installing them. Carnegie class was a significant differentiator regarding perimeter firewall implementation. Eighty-three percent of baccalaureate institutions have installed perimeter firewalls, while only 40 percent of doctoral institutions have installed them.

#### SSL Technology

The most significant difference in technology use among large versus small institutions was in the adoption of Secure Sockets Layer (SSL) for Web transactions. SSL, a commonly used protocol for securing Internet data exchange, is an integral part of most Web browsers and uses a public- and private-

## RECOMMENDATIONS

Based upon its findings in *Information Technology Security: Governance, Strategy, and Practice in Higher Education*, ECAR offers the following recommendations to facilitate more effective IT security on campus:

1. Enlightened policies and procedures contribute to user confidence that academic freedom is being respected. Informing the academic community about IT security policies and demonstrating that the policy is being followed and is trustworthy can alleviate many concerns about security's negatively impacting academic freedom. Having an accepted policy that explains what information the institution collects on its constituents, what the information will be used for, and when it is discarded can calm fears of the user community.
2. An institution must conduct awareness activities for the user community to ensure they understand and trust their IT security policy, and for staff members who configure and use security technologies. An institution might want to periodically audit the information being collected on its users and require business justification for any storage of personally identifiable information.
3. To introduce security standards, IT security personnel must work with faculty and staff to make them aware of the need for security technologies and of its capabilities and limitations. Security personnel must design and implement standards that can accommodate both academic and administrative needs.
4. As the complexity of security issues and technologies grows, and as the time available to deal with threats decreases because of the automated nature of many new attacks, individual departments and research labs within institutions will in many cases have neither the funding nor the expertise to maintain their own IT security. This, in turn, may precipitate a move to more standardized and centralized IT security management at large institutions.

key encryption system, including the use of a digital certificate. More than 83 percent of doctoral institutions employed SSL compared with just 65 percent of other institutions.

### Authentication

All institutions responding to the survey reported using some form of authentication. In addition, 24 percent of the institutions use two forms of authentication, and 50 percent use three or more. The form of authentication used—multiple-use passwords, multilevel passwords, password/PIN combinations, Kerberos, and the like—varies depending on the perceived sensitivity of the data being protected. Nineteen percent of the survey respondents had implemented a single-sign-on system; another 19 percent were currently implementing one; and 48 percent said they plan to implement such a system in the next two years.

### Antivirus Protection

Ninety-seven percent of the surveyed institutions have installed antivirus protection on their operating systems, 90 percent on their application servers, 92 percent on their e-mail servers, and 88 percent on other servers.

### Security Exposure Practices

Sixty-two percent of institutions agreed or strongly agreed that they require all campus-owned computers connected to the network to have known security holes fixed. Fifty-nine percent agreed or strongly agreed that their institutions con-

duct regular and frequent scans to detect known security exposures in critical systems, but only 40 percent agreed or strongly agreed that their institutions conduct regular and frequent scans to detect known security exposures in all campus-owned computers connected to the network.

### Monitoring Networks, Operating and Enterprise Systems, and Routers

Most institutions surveyed monitor their networks (68 percent), operating systems (56 percent), and enterprise systems (62 percent) daily. Larger institutions and doctoral institutions are more likely to monitor on a daily basis. When combined with weekly monitoring, the cumulative percentage rises to 80 percent.

### Incident Response Procedures

Only 19 percent of survey respondents reported that they had had an IT security incident that had been reported in the press. Larger institutions and doctoral institutions were more likely than other institutions to have had an incident reported in the press. As the number of devices and users increases, the percentage of institutions with security incidents reported in the press increases dramatically. Forty-five percent of the institutions have a formal incident-response procedure, with public and doctoral institutions and those with more than 25,000 students most likely to have these procedures in place.