

Roadmap

TOOLS FOR NAVIGATING COMPLEX DECISIONS

Safeguarding the Tower: IT Security in Higher Education 2006

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

KEY FINDINGS

- ▶ From 2003 to 2005, responsibility for IT security moved to the most senior IT leadership—the CIO or specially designated IT security professionals.
- ▶ Compared to 2003, there was significantly less difference in 2005 among Carnegie class institutions in the use of IT security technologies and the provision of awareness programs.
- ▶ Only 46.4 percent of institutions surveyed reported having a disaster recovery plan.
- ▶ A sea change has occurred in two years with respect to centralizing operational staffing structure for central IT security.
- ▶ Departmentally managed systems and data remained at higher IT security risk than those managed centrally.
- ▶ Virtually all institutions had policies on acceptable use of computers, e-mail, Internet, and intranet. The next highest policy coverage was on data backup, access control, authentication and authorization practices, vulnerability management, and physical security.
- ▶ Slightly more than half of the respondents agreed that IT security policies were consistently enforced at their institution.
- ▶ A majority of the institutions in the study had voluntary or mandatory IT awareness programs for students, faculty, and staff. Doctoral institutions were far more likely to have IT security awareness programs.
- ▶ Of the institutions in our study, 42.6 percent had not undertaken a risk assessment in the past two years to determine the value of their IT assets and the risk to those assets. However, the rate of change in undertaking risk assessment from 2003 to 2005 was 76.8 percent.
- ▶ A majority of institutions (74.2 percent) reported that the number of incidents was about the same or less in the past 12 months compared with the year before. There was little variation by Carnegie class.
- ▶ The respondents felt more secure in 2005 than two years earlier, despite being in an environment that is perceived to be riskier.
- ▶ Respondents felt that the academic community has become more sensitive to security and privacy in the previous two years.

Providing secure IT services to colleges and universities is a special, if not unique, challenge. Unfettered and timely access for all to enormous quantities of information is higher education's lifeblood and is key to its success in educating students and generating new ideas and knowledge. Insensitive, political, or casual attempts to check and control this dynamic transmission and consumption of information are problematic at best and potentially deleterious to the academic mission. On the other hand, thoughtful and mission-minded implementation of IT security can and will ensure, protect, and facilitate the requisite flow of information necessary for higher education's continued success. What we find remarkable in

This ECAR roadmap synthesizes the results from a quantitative survey of 492 institutions and interviews with senior IT leaders including members of the EDUCAUSE/Internet2 Computer and Network Security Task Force. The roadmap summarizes the 2006 ECAR study of IT security by Robert B. Kvavik with John Voloudakis. To order the full study or to learn about subscribing to ECAR, visit the ECAR Web site at <http://www.educause.edu/ecar> or contact us at ecar@educause.edu.

KEY REPORT DEFINITIONS

Information security is defined as the preservation of:

- ▀ *Confidentiality*, or protection from unauthorized use or disclosure of information;
- ▀ *Integrity*, ensuring data accuracy and completeness through protection from unauthorized, unanticipated, or unintentional modification, and including authenticity (the ability of a third party to verify that a message's content has not been modified in transit), nonrepudiation (the origin or receipt of a specific message must be verifiable by a third party), and accountability (an action can be traced uniquely to an entity); and
- ▀ *Availability*, making data available to authorized users on a timely basis and when needed.

this longitudinal study of IT security practices in 2003 and 2005 is that in just two years, a balance—or, perhaps more accurately, an acceptable compromise—between these competing interests appears to have been struck at many institutions participating in our study.

There has been a sea change in IT security in higher education in just two years. Of particular note is the growth (22 percent) in the use of firewalls, which many institutions said they were not fond of in 2003. Also significant is the growth in the use of interior firewalls, an increase of more than 27 percent across all Carnegie classes. Other rapidly growing technologies included virtual private networks, up more than 65 percent, and intrusion detection and prevention systems, each up more than 30 percent. We also saw a 55 percent jump in the use of enterprise directories and a nearly 100 percent jump in the use of active filtering technologies. These statistics show that institutions have taken the threat of attack seriously and have taken steps to protect themselves.

Despite significant progress in the use of security technologies, a number of areas can still be improved. Fewer than half of the respondents to this survey were using intrusion prevention systems, 34 percent did not use interior firewalls, and nearly 25 percent did not have centralized data backup capabilities. Fully 95 percent of institutions reported still using traditional username and password combinations. While almost 60 percent indicated they also used strong passwords within their organizations, only 27 percent were using Kerberos, and fewer than 10 percent reported the use of any multifactor authentication mechanism such as hardware tokens (SecureID), biometrics, or PKI.

In 2003, respondents were more focused on technical solutions and put less emphasis on the “softer” aspects of IT security, such as planning, training, auditing, and codifying policies and procedures. The current study

shows tremendous growth rates in the cultural aspects of security. Forty percent of institutions now have a formally designated chief information security officer, up from 22 percent in 2003, and 62 percent of institutions reported having a centralized IT security function, up from only 39 percent in 2003. The number of institutions offering IT security awareness programs jumped by 26.5 percent, with the largest reported program growth targeted at faculty. In the area of planning, we saw a 49 percent rise in institutions that reported having either a partial or complete security plan in place. We saw a 77 percent increase in the number of institutions that had conducted a risk assessment. We also found a substantial reported increase in senior management's interest in IT security issues.

While most respondents had some security policies and procedures in place, there was not uniformity in their coverage. For example, nearly 11 percent did not cover data backup, close to 15 percent did not cover authentication and authorization, nearly 20 percent did not cover physical security, almost 25 percent did not document individual employee responsibilities for security, and more than 30 percent did not cover disaster recovery. More than half of the respondents reported not having formal incident response procedures in place, nearly 50 percent did not test new applications for security, and nearly 70 percent had not established security standards for application or system development. We found that 20 percent of respondents indicated no plan of any type was in place for IT security. Fewer than 10 percent indicated they had undergone a comprehensive risk assessment in the past two years, and more than 40 percent still had not performed any type of risk assessment.

We found that institutions rated the success of their IT security programs lower in 2005 than 2003, although they did rate some aspects of their programs more highly. For example, 15 percent fewer institutions cited lack of

METHODOLOGY

- ▶ A literature review of published works between 2003 and 2005 to create a working set of hypotheses to be tested.
- ▶ Consultation with members of the EDUCAUSE/Internet2 Computer and Network Security Task Force to align the survey with their initiatives and concerns.
- ▶ A quantitative survey of 492 higher education institutions.
- ▶ Qualitative telephone interviews with technology executives, managers, and faculty members.
- ▶ A longitudinal analysis comparing findings from 2003 with those in 2005. Fully 204 institutions responded to both 2003 and 2005 surveys, and we contrast the changes that occurred in that subset of institutions.

awareness as an issue in 2005. The security of central applications, networks, and data was rated much higher than that of locally controlled assets.

The lower rating of overall success comes from several factors. First is the changing nature of threats. As attacks target data rather than systems and networks, the defenses that have been put in place to date are not adequate because they generally are not as strong in the decentralized areas of the organization, where many new attacks are targeted. Also, institutions may have a greater awareness of the complexity of developing a comprehensive security program to combat these changing threats. Added to this is the complexity of managing security in the higher education environment, where many systems are not centrally controlled.

In the 2003 study, one of the key findings was that institutions needed to balance their use of technology with their use of cultural tools to better combat IT security threats. In this study, we see that higher education made significant strides in this area, as well as in technical improvements, and that defenses are more robust than they were several years ago. However, the

disparity found by this study in perceived security between central and local systems, along with the other areas highlighted as possibilities for improvement, now put the spotlight on a new need: development of enterprise security programs designed to protect the entire institution—not just the central systems—and to do so in a coordinated, flexible manner.

Summary

The higher education community has come a long way in two years in accepting prescribed behaviors to make their environments more secure. The culture has changed and done so dramatically. Respondents felt that the academic community has become more sensitive to IT security in the past two years. The security of centrally controlled assets has improved somewhat, but locally controlled assets are still at significant risk. This finding indicates that while a number of specific measures have been implemented to help make institutions more secure, such efforts have not come together into institution-wide programs designed to address the spectrum of threats an institution faces across the full range of institutional IT assets.

TRENDS

- ▶ The world of IT security continues to evolve rapidly, with both the sophistication of threats and the power of tools designed to combat them increasing quickly.
- ▶ Institutions will be under increasing pressure from constituents to provide robust IT security as awareness of its importance rises.
- ▶ 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.

RECOMMENDATIONS

Based on the findings from this study on IT security, ECAR offers the following recommendations to facilitate more effective IT security on campus:

- ▶ 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 they are being followed and can be trusted can alleviate many concerns about IT 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 among the user community.
- ▶ An institution must conduct awareness activities for the user community to ensure that individuals understand and trust the IT security policy and for staff members who configure and use security technologies.
- ▶ To introduce security standards, IT security personnel must work with faculty and their staff to make them aware of the need for security technologies, as well as their capabilities and limitations. IT security staff must design and implement standards that can accommodate both academic and administrative needs.
- ▶ Institutions must continue to take advantage of IT security technologies' new capabilities because, as with any arms race, the tools available to the hacker community are also evolving rapidly.