

5

IT Security Planning and Practice

Planning is bringing the future into the present so that you can do something about it now.

—Alan Lakein

Key Findings

- ◆ The higher its FTE enrollment, the more likely an institution is to have a comprehensive IT security plan and the more likely IT security is to be part of a broader campus plan.
- ◆ While few report a comprehensive IT security plan, the number of respondents having no IT security plan declined dramatically from 2003.
- ◆ More than 60 percent said that IT security was part of a campus or IT strategic plan.
- ◆ Although 42.6 percent of responding institutions had not undertaken an IT security risk assessment in the last two years, we found significant growth in the number that had undertaken a risk assessment from 2003 to 2005.
- ◆ Twenty-five percent of respondents do not perform formal IT security audits.
- ◆ A majority of the respondents require password changes every 180 days or less. One in six respondents does not require password changes.

For IT security programs to be successful, special attention must be paid to security planning, risk assessment, updating and maintaining systems, and password use. Installing technology is no guarantee that it will work as anticipated. Much depends on how, when, and where it is used, by whom, and with what level of effort and skill.

Security Planning

Institutions can be proactive or reactive with respect to IT security. One measure of a proactive security strategy is the preparation of an IT security plan that is comprehensive, monitored, and followed. According to Jack

Suess, vice president of information technology at the University of Maryland, Baltimore County, “Formal security planning focused on procedures and processes will also help improve business continuity planning, overall operations management as well as general reliability planning for critical IT functions.”

A good example of an IT security plan is found at Indiana University. Everything flows from their strategic plan, to activity statements, into specific projects. There are also broad principles about institutional intellectual property and treatment of data (not specifically about technology). The plan dates from 1998.

©2006 EDUCAUSE. Reproduction by permission only.

We asked our respondents whether an IT security plan had been developed and adopted at their institution. We found that 11.2 percent had a comprehensive IT security plan in place, 20.4 percent reported that no IT security plan was in place, and 66.7 percent had a partial plan in place, with 1.6 percent indicating don't know. The higher its FTE enrollment, the more likely an institution is to have a comprehensive plan and the more likely it is that the IT strategic plan is part of a broader campus plan.

In 2003, 44.1 percent of respondents had a partial plan in place and 45.6 percent had no plan or were in the planning stage. Again, we see a sea change in two years in preparedness with respect to IT security, with a 55.6 percent increase in those reporting having partial plans and a 48.6 percent rate of change in the formulation of an IT security plan or partial plan.

Institutions were also asked whether IT security was an integral part of the campus IT strategic plan. We found that 62.5 percent said that IT security was part of a campus or IT strategic plan, 24.6 percent said it was not part of a campus or IT strategic plan, and 10.5 percent had no campus or strategic plan. The remaining 2.4 percent didn't know.

Risk Assessments and Audits

The purpose of a risk assessment is to determine an institution's security requirements on the basis of the actual threats it is facing. According to ISO 17799:2000, the risk assessment should estimate the harm to business that is likely to result from a security failure causing a loss of confidentiality, integrity, or availability of information. It should also estimate the likelihood of a failure occurring, given the current threat environment and the controls currently in place at the institution. Periodic reviews are necessary to accommodate changes to the

institution's academic activities and business operations, to assess new threats and vulnerabilities, and to confirm that current controls are effective and operative. A threat is an adversary who is motivated to exploit a system's vulnerability and is capable of doing so. In summary, risk refers to the likelihood that system vulnerabilities will be exploited and to the potential harm that would be caused were a breach to take place. Note that a risk assessment differs from a vulnerability assessment, which identifies specific errors or weaknesses in a system's design, implementation, or operation.

Risk assessment is increasingly crucial to higher education institutions. As Rob Clark, director of internal auditing at Georgia Tech, observes, "There is not a single process or single organizational unit within the entire campus that would not be literally crippled without the support of its information systems."

According to Indiana University's Mark Bruhn, associate vice president for telecommunications and associate director, IU Center for Applied Cybersecurity Research (and until recently chief IT security and policy officer), "You can't sell IT security on technical merits. You have to sell it in terms of institutional risk. CIOs often try to describe issues to senior executives in terms of specific security vulnerabilities, but they really should focus on risks, operational impacts, and costs. Indiana University has been successful in approaching the board of trustees in this manner."

Others have not fared as well as Indiana University. According to Stanford University's Ced Bennett, emeritus director of information security services, "If an institution makes a really conscious and informed decision not to do a risk assessment, that is fine. Every institution has to decide its risk tolerance or 'risk appetite' and make appropriate decisions about risk. What concerns me is that I don't think most decisions to conduct a risk assessment or not are that conscious or

informed. The decision is more often made based on whether the activity falls 'above or below' the budget line. How does risk assessment compare with an institution's other numerous academic and capital expenditure initiatives? Risk assessment needs to reach the senior administrators' consciousness in a real way. Unfortunately that often occurs only after the shock of a serious incident. Interestingly, many institutions do understand risk assessment related to most other aspects of campus life. For example, they understand about risks to buildings such as fire prevention or the need for supervision and possibly guards at rock concerts, but they view cyber and information risks as just another IT problem (if they think about it at all)."

Another dilemma is finding the necessary skills to conduct risk assessments. Jack Suess, University of Maryland, Baltimore County, tells us, "Risk management is not native to the skill set of most IT organizations. In general, most university IT staff doesn't have formal training on risk assessment and risk management. As organizations reallocate or add staff positions around security, they are trying to identify personnel with an IT security background with risk assessment experience, [and] this often requires looking for people with government or private sector experience."

Ced Bennett supports Suess's comments. "Doing a risk assessment is difficult for many institutions. It is a major project, with an uncertain outcome, and many institutions fail at the 'will' level to get started. Once an institu-

tion has followed accepted methodologies, they find themselves with a result that can be overwhelming, which can paralyze an institution. It does not know what to do next."

The EDUCAUSE/Internet2 Computer and Network Security Task Force Risk Assessment Working Group has created a framework to simplify the risk assessment process and thus make it accessible to a greater number of institutions (see <<http://www.educause.edu/ir/library/pdf/CSD4380.pdf>>).

Fully 42.6 percent of the institutions in our study had not undertaken a risk assessment in the last two years to determine the value of their IT assets and the risk to those assets (see Table 5-1). More than 50 percent of institutions with enrollments under 8,000 had not undertaken some type of risk assessment. We found that 46.3 percent had completed a risk assessment for some institutional data and asset types. Among this latter group, percentages varied from 35 percent or less for institutions with FTE enrollments under 8,000 to over 70 percent for institutions with FTE enrollments above 15,000. Only 8.6 percent of respondents had completed a comprehensive risk assessment. Doctoral institutions are more likely to have undertaken risk assessments and audits.

If we compare findings from 2003 and 2005 for the 204 institutions participating in both studies, we find that 34.0 percent had undertaken a risk assessment in 2003, versus 60.1 percent in 2005—an increase of 76.8 percent.

Table 5-1. Risk Assessment in the Last Two Years (N = 488)

	Number	Percentage
No risk assessments done	208	42.6%
For some institutional data and asset types	226	46.3%
For all institutional data and asset types	42	8.6%
Don't know	12	2.5%

According to Georgia Institute of Technology's director of internal auditing, Rob Clark, "There is an increased level of awareness regarding IT issues and IT risk, and that particularly business managers are paying more attention to these issues. In the past, dealing with IT risk had been traditionally relegated to the IT department. But it's now clear from communications, case studies, and high-profile examples that business officers need to be involved in the IT risk assessment process. High-profile incidents have also shown that internal auditors need to focus on IT risk assessment as well as compliance and traditional financial controls."

Clark further comments, "Many institutions have not yet dedicated the resources to conduct a thorough IT risk assessment. Many senior managers are aware and understand the importance of assessing IT risks but fall short in doing so for several reasons: budgets have not been established to delineate IT risk assessment as a specific funded item or initiative; the cost of conducting an IT risk assessment is unknown; and it's unclear how it will be accomplished, given stretched resources."

Jack Suess predicts that risk assessments and formal processes will become increasingly commonplace for many institutions. They are mandatory now as a result of HIPAA and Graham-Leach-Bliley. "If I look into the crystal ball I believe that by 2010 most, if not all, institutions will have to implement formal risk assessment methodologies because of

mandates by their board or an outside body. If you use the time now to prepare your organization, you will have a better chance of success if this becomes required." He adds, "My campus is two years away from implementing a formal risk assessment methodology. I am trying to prepare the campus to move in this direction by rolling out a broad risk assessment process that involves the IT staff on the campus as well as the executives. These steps are preparatory to get us to a point where we can create a culture around a formal security methodology."

We asked about the frequency of formal IT security audits (see Table 5-2). Twenty-five percent do not perform IT security audits. The majority (50.6 percent) perform audits on an irregular basis. The smaller the FTE enrollment, the less likely an institution is to perform an audit. The range varied from 40.0 percent of institutions with FTE enrollments under 2,000 not performing audits to 6.1 percent of institutions not performing audits with FTE enrollments above 25,000. Note also that only 18.9 percent of institutions provide departments with a framework for performing IT security assessments. This service is more likely at doctoral institutions and four times more likely at institutions with higher FTE enrollments, but the numbers remain low and did not change significantly between 2003 and 2005.

We asked who participated in the audits (see Table 5-3). Internal IT staff (72.6 percent) performed most audits, followed by

Table 5-2. Frequency of Formal IT Security Audits (N = 492)

	Number	Percentage	Cumulative Percentage
Not performed	123	25.0%	25.0%
On an irregular basis	249	50.6%	75.6%
On a regular basis	113	23.0%	98.6%
Don't know	7	1.4%	100.0%

an external auditor (65.5 percent), and the IT security officer (62.7 percent). Least used were external consultants (28.9 percent) and vendors (22.2 percent).

A clear change from 2003 to 2005 is the use of external auditors and external consultants to conduct IT security audits (see Table 5-4). This is especially the case at institutions with higher FTE enrollments.

At a far simpler level, but equally important, is identifying and correcting infections on machines using the university network. The George Washington University, according to Krizi Trivisani, systematically identifies infected student systems. "We implemented Cisco Clean Access in our student network in August 2005 to alleviate the problems associated with incoming students' accessing the network with unsecured machines. After Clean Access, the numbers dropped from

800 infected machines to 65 machines at the beginning of the semester. We used to have 100 to 150 new infections per month; now it is less than 10 per month."

Updating and Maintaining Systems

We asked institutions whether their implementation protocol requires all new enterprise systems and applications to be tested for IT security. In 2003, we found that 52.2 percent of the respondents required testing and 45.8 percent did not. This compares with 46.0 percent requiring testing and 49.5 did not in 2003. The rest didn't know.

We also asked about the frequency of testing enterprise systems for IT security (see Figure 5-1). Because of coding changes in the 2005 survey, we cannot map the rate of change from 2003.

Table 5-3. Who Conducts IT Security Audits? (N = 492)

Participant	Percentage
IT staff	72.6%
External auditor	65.5%
IT security officer	62.7%
Internal auditor	45.3%
External consultant	28.9%
Vendor	22.2%

Table 5-4. Change in Auditors and External Consultants, 2003 to 2005 (N = 204)

Participant	2005	2003	Percentage Change	Rate of Change
External auditor	63.8%	53.6%	10.2%	19.0%
Internal auditor	53.8%	50.0%	3.8%	7.6%
External consultant	46.3%	32.1%	14.2%	44.2%
Vendor	22.8%	21.5%	1.3%	6.0%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Changing Passwords

We asked institutions how often passwords were required to be changed (see Table 5-5). A majority of the respondents said every 180 days or less (57.2 percent); 16.5 percent had no requirement. Because of coding changes in the 2005 survey, we cannot map the rate of change from 2003.

Summary

As with technologies in use and awareness programs, planning, audits, and risk assessments are all up significantly from 2003. This has occurred across all higher education sectors to the point where differences among institutions are minimal. In this area, higher education has made breathtaking progress.

Figure 5-1.
Frequency of
Testing Enterprise
Systems for IT
Security (N = 489)

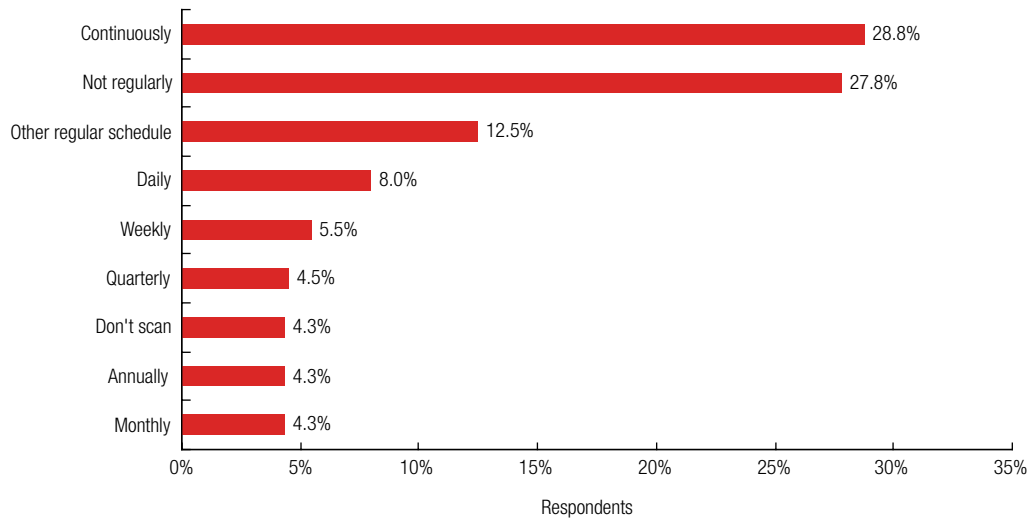


Table 5-5. Frequency of Password Changes (N = 474)

	Number	Percentage	Cumulative Percentage
Single use	2	0.4%	0.4%
Every 30 days	18	3.8%	4.2%
Every 60 days	53	11.2%	15.4%
60–180 days	198	41.8%	57.2%
More than 180 days	28	5.9%	63.1%
It varies	90	19.0%	82.1%
No requirement	78	16.5%	98.5%
Don't know	7	1.5%	100.0%