

4

Organization, Leadership, Policies, and Awareness

We can't solve problems by using the same kind of thinking we used when we created them.

—Albert Einstein

Key Findings

- ◆ While 67 percent of research universities report having a chief IT security officer, only 20 percent of other respondents report having one.
- ◆ The position of chief IT security officer is full time at 32.2 percent of the institutions in our study, up from 20.0 percent in 2003. Of the full-time IT security officers, 70.6 percent work at doctoral institutions.
- ◆ Responsibility for IT security has moved toward chief security officers and CIOs and away from directors of networking and other IT management.
- ◆ Eighteen percent of our survey respondents indicated that the person in charge of IT security holds IT security certification. More than 20 percent of all IT security staff had earned certification.
- ◆ Nearly one-third of respondents expect to increase their IT security staff.
- ◆ An additional one-quarter of the 204 institutions in the 2003 and 2005 surveys have centralized security in the IT organization, and the rate of change was 59.7 percent.
- ◆ There has been significant growth in the scope of policies in place among respondents.
- ◆ Most respondents do not believe that IT security is part of the institutional culture, but they do believe that improvement has taken place since 2003.
- ◆ Slightly more than half of respondents agreed that IT security policies were consistently enforced at their institution.
- ◆ Most respondents report having IT security awareness programs for students, faculty, and staff. Doctoral institutions are far more likely to have such programs.
- ◆ On average, institutions plan to spend most of their IT budgets on security products and training, followed by services and staffing.

Every IT security solution requires attention to both technology and the people who use it. Shirley Payne, director of security coordination and policy at the University of Virginia, says, "Don't focus on technical solutions at the

expense of user education. Many incidents occur because of human error. For this reason it's vital to have an effective program in place to build and maintain a security-aware culture, in addition to implementing technology-based

©2006 EDUCAUSE. Reproduction by permission only.

safeguards.” She adds, “Focus on transferable principles. Teach principles and not technology. Technology keeps changing—first laptops, then PDAs, and now thumb drives. If people understand the need to protect their data in ever-changing computing environments, then the medium they use becomes less important. They transfer the basic principles to whatever type of device they are using.”

We share the position espoused by Payne and the Government Accountability Office (GAO) that system security is a holistic problem, with technological, managerial, organizational, regulatory, economic, and social aspects interacting. We discussed technical approaches to IT security in Chapter 3. We focus here on the human dimension of security and its foundation, paying particular attention to organization, leadership, policies, and university community awareness of IT security.

Managing IT Security on Campus

The Gramm-Leach-Bliley Act of 1999 as interpreted by the Federal Trade Commission in 2002 mandates that higher education institutions designate an individual to be responsible for IT security for financial transactions. The act doesn’t specify title; the job doesn’t have to be full time; where the position reports is an internal institutional matter.

Ced Bennett, emeritus director of information security services at Stanford University, reinforces this position: “There has to be someone who thinks about IT security from an institutional viewpoint in addition to those who must pay attention to security from some specific compliance perspective related to particular data such as student financials.”

Our survey asked if someone had chief responsibility for IT security, that person’s title, when the position was created, the reporting relationships, skills, and experience. We found that 34.9 percent of the respondents indicated that their institution had a formally designated

individual as its IT security officer, with 55.5 percent of them having been appointed since 2003. In 2003, only 15.5 percent of the institutions in the ECAR study formally designated an individual as their IT security officer.

The vast majority of IT security leaders with day-to-day management responsibility for IT security (98.8 percent) hold their position in the IT organization (see Table 4-1). This is up slightly from 95.9 percent in 2003. Fully 67.4 percent of these individuals work full time on IT security. The position titled IT security officer is most often in charge of IT security (34.9 percent), followed by the director of networking (21.8 percent). The notable difference among Carnegie class institutions is the prominence of an IT security officer at doctoral institutions (67.2 percent, up from 52.0 percent in 2003), versus fewer than 20 percent at other institutions. The director of networking and the CIO play the dominant role at all other Carnegie class institutions.

The position of chief IT security officer is full time at 32.2 percent of the institutions in our study, which is up from 20.0 percent in 2003. In the United States, 70.6 percent of the full-time IT security officers work at doctoral institutions.

IT security officer reported salaries average between \$75,000 and \$99,000. In two years, the average salary for this position has moved from the \$50,000–\$74,000 range to the \$75,000–\$99,000 range. Not unexpectedly, the salaries for IT security officers at doctoral institutions are highest, followed very closely by those at MA institutions.

We were interested in whether the responsibility for IT security had changed in the last two years (see Table 4-2). We found that responsibility had moved toward chief security officers (55.8 percent rate of change) and CIOs (113.4 percent rate of change) and away from directors of networking (–28.8 percent rate of change) and other IT management (–22.7 percent rate of change). Indeed, all of the positive

Table 4-1. Position with Day-to-Day Responsibility for IT Security (N = 490)

Position	Number	Percentage
IT security officer	171	34.9%
Director of networking	107	21.8%
Other IT management	82	16.7%
CIO	70	14.3%
Other IT non-management	35	7.2%
Director of administrative computing	13	2.7%
Director of academic computing	6	1.2%
Other administrative management	3	0.6%
Other academic management	3	0.6%

Table 4-2. Change in Positions with Day-to-Day Responsibility for IT Security, 2003 to 2005 (N = 204)

Position	Percentage Responsible in 2005	Percentage Responsible in 2003	Percentage New Adopters	Rate of Change 2003–2005
IT security officer (or equivalent)	34.9%	22.4%	12.5%	55.8%
CIO (or equivalent)	14.3%	6.7%	7.6%	113.4%
Director of administrative computing	2.7%	3.2%	–0.5%	–15.6%
Director of academic computing	1.2%	1.8%	–0.6%	–33.3%
Other academic management	0.6%	1.2%	–0.6%	–50.0%
Other administrative management	0.6%	3.2%	–2.6%	–81.3%
Other IT management	23.9%	30.9%	–7.0%	–22.7%
Director of networking	21.8%	30.6%	–8.8%	–28.8%

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

movement has been toward the positions of chief IT security officer and the CIO. This finding reflects the ever-increasing visibility of IT security as a means of countering threats to the institution. According to Krizi Trivisani, director of systems security operations and chief security officer at The George Washington University, “CIOs need a dedicated CSO who does this

for a living. Security is just one aspect of IT and it is very specialized. The CSO needs to stay ahead of the issues and needs the funding and political clout to get the information out there.”

It is useful to look at the shift of responsibility for IT security to the CIO and IT security officer by institution size, measured by FTE enrollments (see Table 4-3). Institutions with en-

rollments over 25,000 have almost completely delegated the responsibility to an IT security officer. Clearly it is with these institutions that most of the change has occurred from 2003 to 2005. As FTE enrollment declines, so does the position of IT security officer, to 13 percent or less at institutions with FTE enrollments of 4,000 or fewer. We see a reverse pattern with the positions of CIO and director of networking. Moreover, as FTE enrollments decrease, full-time effort by the individual assigned primary responsibility for IT security declines from 81.8 percent to 9.5 percent.

University of Maryland, Baltimore County's Jack Suess provides an interesting perspective on IT security staffing. "It is a positive thing that more and more institutions have hired an information security officer. But I worry that IT security can become its own silo. Unless we

embed security throughout the entire IT organization and campus, we are not going to be successful in securing our campus IT infrastructure. CIOs must make IT security a team-based approach. The information security officer is the key member of a team that includes representatives from networks, application development, system administration, user support, and key departments that run large systems with private data. The CIO has to bring those people together regularly and foster a culture around security. Within institutions—especially within IT—everyone has a role to play in securing the infrastructure, and security should be a part of each staff member's performance evaluation. We will know we are on the path to success when our campus leaders are prepared to also say security is part of everyone's job on campus." Note, however, that it is

Table 4-3. Position with Day-to-Day Responsibility for IT Security, by FTE Enrollment (N = 471)

Position	FTE Enrollment						Total
	1–2,000	2,001–4,000	4,001–8,000	8,001–15,000	15,001–25,000	More Than 25,000	
CIO (or equivalent)	26.6%	16.0%	14.0%	5.3%	6.7%	6.1%	14.4%
IT security officer (or equivalent)	11.9%	13.0%	36.6%	52.6%	53.3%	87.9%	34.2%
Director of administrative computing	3.7%	2.0%	4.3%	1.3%	1.7%	0.0%	2.5%
Director of academic computing	1.8%	3.0%	0.0%	1.3%	0.0%	0.0%	1.3%
Director of networking	30.3%	35.0%	20.4%	14.5%	11.7%	0.0%	22.3%
Other IT management	13.8%	18.0%	20.4%	14.5%	25.0%	3.0%	16.8%
Other IT non-management	10.1%	11.0%	3.2%	9.2%	1.7%	3.0%	7.2%
Other administrative management	0.0%	1.0%	1.1%	1.3%	0.0%	0.0%	0.6%
Other academic management	1.8%	1.0%	0.0%	0.0%	0.0%	0.0%	0.6%
Total Institutions	109	100	93	76	60	33	471

incumbent on every institution to have someone in charge with the authority to make final decisions and be held accountable for results.

To Whom Does the IT Security Position Report?

We found that 54.2 percent of IT security officers report to the CIO and 80.7 percent to an IT officer (see Table 4-4). Fully 18.3 percent report to a non-IT officer. There was little change between 2003 and 2005. And there was little difference by Carnegie class or institutional FTE enrollment.

IT Security Certification

IDC reports that the market for security education and training will have 16.4 percent year-over-year growth reaching approximately \$1.6 billion by 2009 (Carey, 2005). This is in part a response to the incredible pace of change within IT security technologies and architecture. IDC reports that 60 percent of the IT professionals surveyed planned on taking an additional certificate in the next 12 months.¹

Carol Myers, CIO at Paradise Valley Community College, noted a significant three-year increase in the number of certifications

available, including certification from Cisco, Microsoft, Novell, and Sun. She expects further growth as state and federal agencies increasingly require certification. Also noted were pay incentives for individuals acquiring certification. Marilu Goodyear, associate professor of public administration and former CIO at the University of Kansas, notes pressure from university counsel offices and law enforcement, who prefer certified people for court appearance in cases such as data compromise and criminal pornography charges. Goodyear also notes that certification is sometimes not successful in upgrading individuals' skills in the eyes of their colleagues. That opinion squares with comments made by Ced Bennett at Stanford University: "Certification is pursued largely by those who focus on the specific details of security implementation." In his opinion, ownership or lack of ownership of any of the major certifications is only one factor in determining actual professional competency.

Eighteen percent (91) of the respondents in our survey indicated that the person in charge of IT security holds one IT security certificate. Three percent (16) of those in charge of IT security hold two certificates,

Table 4-4. To Whom Does the IT Security Officer Report? (N = 487)

Position	Number	Percentage
CIO (or equivalent)	265	54.2%
Other IT management	59	12.1%
Vice president/vice provost (non-CIO)	58	11.8%
Director of networking	36	7.3%
Chancellor/president/provost	32	6.5%
Director of administrative computing	25	5.1%
Director of academic computing	6	1.2%
Other administrative management	3	0.6%
Other academic management	2	0.4%
Other IT non-management	1	0.2%

and three percent (17) hold three. Six hold four or five certificates. As shown in Figure 4-1, of the individuals who have certification, 15.3 percent (72) hold the Certified Information Systems Security Professional (CISSP) certificate. Five and a half percent (25) hold the Certified Information Security Manager (CISM) certificate, 5.2 percent (24) hold the Global Information Assurance Certification (GIAC), and 2.4 percent (11) hold the Certified Information Systems Auditor (CISA) certificate. We found that 14.9 percent hold other security certifications. The home institution most often awards these as part of their ongoing training program.

When asked how many of their institution’s IT security staff had earned certification, the respondents reported 20.5 percent. We found that 8.6 percent of the respondents reported that two of their IT staff had certificates, and 4.3 percent reported having three staff with certificates. Four respondents reported that they had 10 or more staff with certificates.

In 2003, more than half of the certificate recipients were situated at doctoral institutions. This is not the case in 2005: MA institutions in this study have 31.5 percent of the

certificate holders, versus 29.1 percent for the doctoral institutions. However, the larger the FTE enrollment, the more likely it is that individuals will hold a certificate. For example, at institutions with an enrollment of 4,000 or fewer, 6.9 percent hold a CISSP certificate, versus 39.4 percent at institutions with FTE enrollments over 25,000. We found that the position most likely to hold a certificate was the IT security officer, which held 34.9 percent of all certificates, followed by the director of networking at 21.8 percent. CIOs held 14.3 percent of the certificates.

We compared the change in percentage of certificate holders by looking at what happened at the 204 institutions in the 2003 and 2005 studies (see Table 4-5). Clearly the percentage of certificate holders is up, especially for the CISSP—a change of 67.7 percent. While the rate of change is high for the GIAC and the CISA, the actual percentage of certificate holders is low.

Staffing and Staffing Trends

The 2005 EDUCAUSE core data survey queried respondents on the size of their IT

Figure 4-1.
Security Certificates Held by IT Security Staff

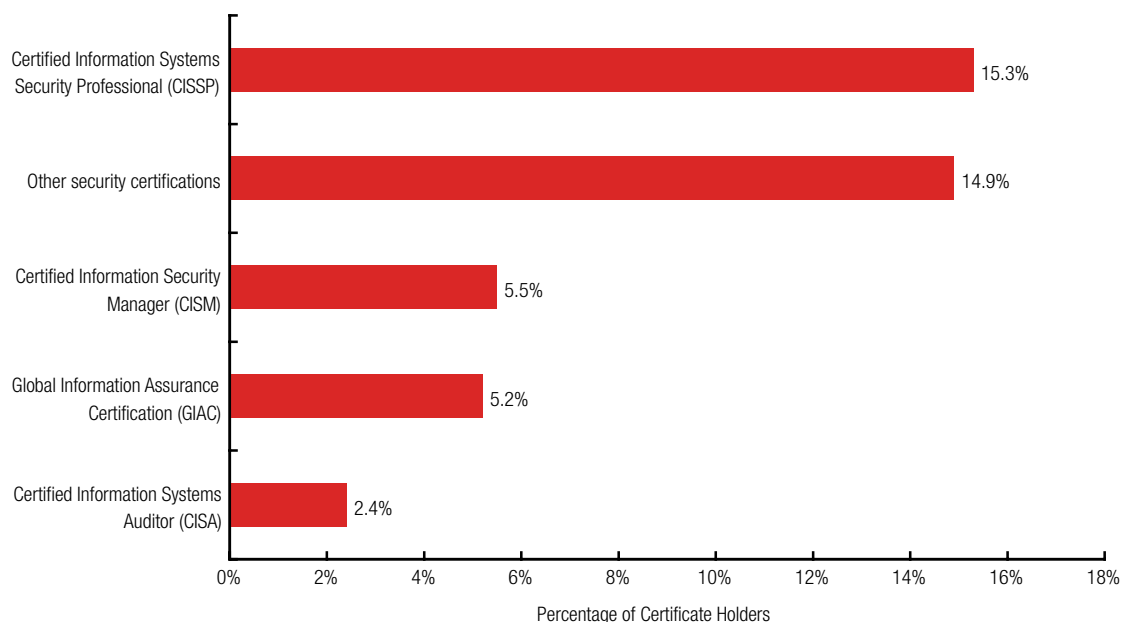


Table 4-5. Change in Certification from 2003 to 2005 at 204 Institutions

Certificate	Percentage Held in 2005	Percentage Held in 2003	Percentage New Holders	Rate of Change 2003–2005
Certified Information Systems Security Professional (CISSP)	20.8%	12.4%	8.4%	67.7%
Global Information Assurance Certification (GIAC)	6.8%	2.6%	4.2%	161.5%
Certified Information Systems Auditor (CISA)	3.2%	1.5%	1.7%	113.3%

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

Table 4-6. Average Number of Regular IT Security Staff, by Carnegie Class

Carnegie Class	FTE Staff
Other	0.7
AA	0.2
BA	0.3
MA	0.6
DR	2.8
All	1.1

security staff (see Table 4-6). The average number of full-time staff is provided for each Carnegie class. Clearly, doctoral institutions employ the most IT security staff (2.8 FTEs).

We found a higher number of central FTE IT security staff on average at all institutions than was reported to the 2005 core data survey. We found that 39.4 percent have less than one full-time employee managing security, 21.4 percent have one FTE, 13.6 percent have two employees, 7.8 percent have three employees, and 4.7 percent have 10 or more employees (see Table 4-7). Note, too, that doctoral institutions have a larger staff. More than 68 percent of the MA, BA, and AA institutions report that they have a security staff of one or less than one, whereas 62 percent of the doctoral institutions report

that they have a staff of more than two.

We were also interested in any change in the size of the IT security staff from 2003 to 2005 at the 204 institutions in both studies (see Table 4-8). Noteworthy is a negative 14.2 percent change in having less than one FTE. In almost every instance, the size of the staff is increasing, though the growth is mainly at doctoral institutions. Again, this likely demonstrates the increasing visibility of the IT security problem, as more institutional resources are being allocated to this area.

Ced Bennett notes, “More institutions recognize the need for IT security staffing now. There are more people who are being assigned to security as a primary job instead of it being just a part of a system administrator’s

Table 4-7. Size of Central IT Security Staff, by Carnegie Class (N = 411)

Staff Size	DR	MA	BA	AA	Total
Less than 1	7.6%	45.7%	69.0%	44.7%	39.4%
1	11.8%	29.5%	20.7%	23.7%	21.4%
2	18.5%	16.3%	3.4%	13.2%	13.6%
3	17.6%	3.1%	3.4%	5.3%	7.8%
4	10.1%	0.8%	1.1%	2.6%	3.9%
5	9.2%	1.6%	0.0%	3.9%	3.9%
6 or more	25.2%	3.1%	2.3%	6.6%	10.0%

Table 4-8. Change in Size of Central IT Security Staff, 2003 to 2005 (N = 204)

Staff Size	2005 Percentage	2003 Percentage	Percentage Change	Rate of Change
Less than 1	31.9%	46.1%	-14.2%	-30.8%
1	21.6%	20.6%	1.0%	4.9%
2	14.2%	11.8%	2.4%	20.3%
3	8.3%	9.8%	-1.5%	-15.3%
4	5.9%	4.9%	1.0%	20.4%
5	4.9%	2.0%	2.9%	145.0%
6 to 10	9.8%	4.4%	5.4%	122.7%
More than 10	3.4%	0.1%	3.4%	3,300.0%

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

duties. I see institutions which had no allocation for IT security which are now putting real resources into it.”

We asked institutions to indicate whether they anticipated changes in the number of IT security employees within the next two years (see Table 4-9). Fewer than 1 percent (two institutions) indicated an expected staff decrease (both have FTE enrollments of 4,000 or fewer), while 50.2 percent expected no change, 24.4 percent expected to add one staff member, and 7.7 percent expected to add two or more. The anticipated increases are largely at doctoral institutions and institutions with higher FTE enrollments. These expectations mirror what

was reported in 2003, and the percentage changes reported in Table 4-8 suggest that the expectations came true.

IT Security Organization

The IT security literature recommends the establishment of a central security office. According to the GAO, in its May 1998 *Executive Guide, Information Security Management, Learning from Leading Organizations*, the advantage is that central groups can

- ◆ serve as catalysts for ensuring that information security risks are considered in both planned and ongoing operations;
- ◆ provide advice and expertise to units

Table 4-9. Expected Increase in Size of Central IT Security Staff (N = 492)

Expected Staff Increase	Number	Percentage	Cumulative Percentage
Increase by more than two FTE staff	15	3.0%	3.0%
Increase by two FTE staff	23	4.7%	7.7%
Increase by one FTE staff	120	24.4%	32.1%
Stay the same	247	50.2%	82.3%
Decrease by one FTE staff	2	0.4%	82.7%
Don't know	85	17.3%	100.0%
Total	492	100.0%	

- throughout their institution;
- ◆ keep top management informed about security-related issues and activities affecting the organization;
- ◆ achieve some efficiency and increase consistency in the implementation of the organization's security program by performing tasks centrally that might otherwise be performed by multiple individual business units;
- ◆ provide training;
- ◆ research potential threats, vulnerabilities, and control techniques and communicate this information to others in the organization;
- ◆ monitor various aspects of the organization's security-related activities by testing controls, accounting for the number and types of security incidents, and evaluating compliance with policies;
- ◆ establish a computer incident response capability and, in some cases, serve as members of the emergency response team;
- ◆ assess risks and identify needed policies and controls for general support systems, such as organization-wide networks or central data processing centers;
- ◆ create standard data classifications and related definitions to facilitate protection of data shared among two or more busi-

- ness units;
- ◆ review and test the security features both in commercially developed software being considered for use and in internally developed software prior to its being moved into production; and
- ◆ provide self-assessment tools to business units so that they can monitor their own security posture.

Our data confirm the GAO's assertion: Institutions with a dedicated security staff are more likely to fulfill the above functions. This was a major finding of the 2003 study.

Centralized and Decentralized Offices

Our data show that 61.8 percent of the total respondents have one central IT security unit, while 32.7 percent spread the responsibility across multiple IT units. We found that 5.5 percent specified other or don't know.

A sea change has occurred in two years with respect to the operational staffing structure for central IT security (see Table 4-10). An additional one-quarter of the 204 institutions in the 2003 and 2005 studies have moved to centralize security in the IT organization, and the rate of change was 59.7 percent. Much of that change occurred in doctoral institutions. For the 204 institutions in 2005, there appears

Table 4-10. Change of Operational Staffing Structure for IT Security, 2003 to 2005 (N = 204)

Staffing Structure	2005 Percentage	2003 Percentage	Percentage Change	Rate of Change
One central IT security unit/function	61.8%	38.7%	23.1%	59.7%
Spread across multiple central IT units/functions	32.7%	58.2%	-25.5%	-43.8%
Other	5.5%	3.1%	2.4%	77.4%

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

to be little difference by Carnegie class or by FTE enrollment. Again, this shows the growing importance of IT security to the institution. We note, however, that decentralization remains an issue in all institutions in our study. While centralization of responsibility has occurred within the central IT organization, colleges and other administrative units that manage separate IT organizations and technologies continue to challenge overall IT security, as detailed in Chapter 7. Chapter 8 discusses approaches institutions can use to mitigate the impact of decentralized units on overall enterprise security.

Security Policy

According to the GAO, "The framework within which an organization strives to meet its needs for information security is codified as security policy. A security policy is a concise statement, by those responsible for a system (e.g., senior management), of information values, protection responsibilities, and organizational commitment." A good security policy can play an important role in liability abatement, as it demonstrates that the institution has taken appropriate and necessary precautions to protect its information assets and its clients. It also serves to educate the population as to what is expected of them vis-à-vis security. As we found in the 2003 ECAR study, end users generally want to help the institution stay secure, but they often don't know how. Having a well-

documented, easily accessible policy gives users a place to turn if a question arises.

Policies on Campus

Where and when have security policies been implemented? Who was involved in their development? What policies have institutions put into place regarding access to and usage of their networks, computing resources, applications, and data/information resources? Are these policies enforced and updated?

Table 4-11 shows the percentage of institutions that have implemented specific policies. Virtually all institutions (97.8 percent) have policies on acceptable use of computers, e-mail, Internet, and intranet. The next highest coverage is on data backup, access control, authentication and authorization practices, vulnerability management, and physical security. We found that 38.1 percent of institutions have policies on personnel clearance or background checks. Note that the policies we identified in 2005 do not map to policies identified in the 2003 survey.

With the exception of security compliance monitoring, which was higher at doctoral institutions, there was little difference by Carnegie class. Institutional size measured by FTE enrollments made a difference on data classification, retention, and destruction (40.0 percent at institutions with enrollments 4,000 or fewer and 69.0 percent at institutions with FTE enrollments over 15,000);

Table 4-11. Security Policies Implemented (N = 491)

Policy Implemented	Percentage
Acceptable use of computers, e-mail, Internet, and intranet	97.8%
Data backups and secure off-site storage	89.1%
Access control, authentication, and authorization practices	85.1%
Vulnerability management (such as patch management or antivirus software)	85.1%
Physical security	81.4%
Individual employee responsibilities for information security practices	72.8%
Protection of organizational assets	72.8%
Managing privacy issues, including breaches of personal information	71.6%
Secure disposal of data, media, or printed material that contains sensitive information	71.0%
Incident reporting and response	68.9%
Disaster recovery contingency planning (business continuity planning)	68.4%
Investigation and correction of the causes of security failures	68.2%
Notification of security events to affected parties (individuals, law enforcement, campus organizations)	66.9%
Sharing, storing, and transmitting of institutional data (such as ISPs, external networks, or contractors' systems)	51.3%
Data classification, retention, and destruction	50.6%
Identity management	50.0%
Security compliance monitoring and enforcement	49.0%
Change management processes	45.6%
Personnel clearances or background checks	38.1%

disaster recovery (60.6 percent at institutions with enrollments 4,000 or fewer and 75.8 percent at institutions with FTE enrollments over 15,000); incident reporting (52.3 percent at institutions with enrollments 4,000 or fewer and 90.0 percent at institutions with FTE enrollments over 15,000); security compliance and monitoring (40.7 percent at institutions with enrollments 4,000 or fewer and 63.6 percent at institutions with FTE enrollments over 15,000); and notification of security events to affected parties including individuals, law enforcement, and campus

organizations (54.1 percent at institutions with enrollments 4,000 or fewer and 93.9 percent at institutions with FTE enrollments over 15,000). In short, we note significant differences in the scope of policies in place at institutions with higher FTEs. However, policy enforcement does not vary much by institution size.

Work is ongoing to clarify what each policy should contain. With respect to incident handling procedures, the 2005 Cybersecurity Summit at Tysons Corner, Virginia, noted that "in many cases it was unclear if a site

should contact a user directly, or a system administrator at the site the user was coming from, or both. In cases where a user used a compromised host to access another site, it is unclear whose responsibility it is to inform the remote site of their compromised system. Should the user or security staff?"

We were also interested in whether the IT security policies were consistently enforced and updated (see Tables 4-12 and 4-13). Slightly more than half of the respondents agreed that IT security policies were consistently enforced at their institution (mean of 3.40, where 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree), while the group divided equally on updating of policies (mean of 3.33).

IT Security Awareness

Is the campus community well educated about security risks? Are awareness pro-

grams and practices in place? For whom, and are they effective? This issue is critical, as many believe that the greatest risk to the institutions is internal. While most internal users are not ever going to try to maliciously compromise the institution's systems, many security issues arise when an internal user inadvertently compromises security—for example, by not installing an operating system patch or by giving the user's password to someone over the phone.

Continual security education is likely one of the most cost-effective and important defensive strategies an institution can take. Toward this goal, institutions can consult any of the numerous helpful Web sites cited in Appendix C. For example, one page at the SANS Institute Web site <<http://www.sans.org/resources/mistakes.php>> details common mistakes people make that lead to security problems.

Table 4-12. IT Security Policies Are Consistently Enforced (N = 490)

	Number	Percentage
Strongly disagree	6	1.2%
Disagree	84	17.1%
Neutral	137	28.0%
Agree	226	46.1%
Strongly agree	33	6.7%
Don't know	4	0.8%

Table 4-13. IT Security Policies Are Regularly Updated (N = 490)

	Number	Percentage
Strongly disagree	6	1.2%
Disagree	98	20.0%
Neutral	141	28.8%
Agree	213	43.5%
Strongly agree	30	6.1%
Don't know	2	0.4%

Awareness is also a moving target, which makes for difficulty in keeping the community abreast of the latest risks to their equipment and software. The George Washington University's Krizi Trivisani notes, "You need to hit hard on the issues facing the organization at a particular time. Security threats change so rapidly, it can be difficult to maintain awareness on current issues. Last year's training focus was identity theft; this year's focus is laptops and encryption."

In a similar vein, Tracy Mitrano, director of IT policy and computer policy and law programs at Cornell University, observes a shift of IT security from devices to data: "We recognize the vulnerability of sensitive data. We've also been able to leverage awareness in the general community to the needs of IT security because of their interest in data breach, state notification laws, and identity theft." She further notes, "In the age of information, one of the most popular crimes appropriates information for criminal purpose. If booze defined the Gatsby 1920s, information defines the crime of this era."

IT Security as an Institutional Priority

We asked respondents whether IT security was one of the top three issues confronting their institution today. We found that 80.6 percent agreed or strongly agreed (up from 75.0 percent in 2003), 10.8 percent were neutral, 7.7 percent disagreed or strongly disagreed, and 0.8 percent did not know. Institutions with higher FTE enrollments were more likely to strongly agree. In 2003, doctoral institutions rated this a higher-priority issue than other Carnegie classes. In 2005, BA institutions gave this a slightly lower priority, while all other classes and Canadian institutions looked very similar.

We were also interested in whether IT security practices are woven into the fabric of the institution's business practices and

whether IT security is part of the institution's employee culture. Only 33.9 percent agreed or strongly agreed that IT security practices were woven into the fabric of their institution's business practices. This percentage is virtually unchanged from 2003. And 25.5 percent agreed or strongly agreed that IT security is part of the institutional employee culture; more than half disagreed or strongly disagreed. AA institutions score slightly higher on these two dimensions and BA institutions slightly lower. FTE enrollment size did not make a difference.

Awareness Communication Programs

The number of institutions with awareness programs has significantly increased since 2003. EDUCAUSE has helped this effort by providing materials and resources, as well as training at different conferences. At The George Washington University, Krizi Trivisani uses the following approach: "We hit key people in the organization who can be champions on security within their groups. We do a variety of awareness training—online training for basic issues, brown-bag sessions about specific issues, deploy EDUCAUSE's executive awareness video, and hold monthly meetings for our local support partners." Of special interest is their contest called PatchaPaloosa (copyright Blaine A. D'Amico, game developer). "Currently we use PatchLink—a multiplatform security patch, vulnerability assessment, and compliance management solution—to patch our systems. Our contest has a horse race motif. Every local support partner has a jockey for his or her department or area. The goal is to increase the percentage of computers patched with PatchLink in each area. The area with the largest percentage of patched machines—a minimum of 65 percent fully patched is required for every area—receives a vendor-donated award such as a high-end color or black-and-white printer. There is a lot

involvement and information distribution to the users. It creates excitement and gets the word out. We have seen significant increases in our patched levels from this awareness activity.”

In 2003, we learned that awareness programs were as critical as installed technologies in ensuring that IT security was attained. We again queried whether institutions communicate IT awareness issues to their faculty, students, and staff on a regular basis (see Table 4-14).

We found that 51.1 percent were neutral, disagreed, or strongly disagreed. If we look at the 204 institutions in the 2003 and 2005 studies, IT security awareness programs have increased by 26.5 percent. BA institutions were slightly less likely to communicate IT security awareness than other Carnegie class institutions. And institutions with smaller FTE enrollments were less likely to communicate awareness issues. Carol Myers, CIO at Paradise Valley Community College, notes a greater awareness of the need for IT security in the last three years, including among senior administrators, although she still recognizes a need for more improvement, especially by deans and other managers.

A majority of the institutions in the study had voluntary or mandatory IT awareness programs for students, faculty, and staff (see Table 4-15). Doctoral institutions are far more likely to

have IT security awareness programs (nearly 80 percent), versus fewer than 50 percent at other Carnegie class institutions. Half of the institutions in the study with FTE enrollments of fewer than 8,000 had no awareness program, versus 15.2 percent of the institutions with FTE enrollments over 25,000. Noteworthy is the finding that the majority of IT security awareness programs are voluntary, especially for faculty. We also find that the largest percentage of no programs available affects students.

Table 4-16 indicates that the number of awareness programs offered by the 204 institutions in the 2003 and 2005 studies has grown significantly—an increase of more than 25 percent.

Krizi Trivisani forecasts, “Lack of training is not going to be an excuse anymore. It will be considered negligent if an institution does not provide awareness training to their employees and staff. Awareness and training is evolving from an important issue to a critical success factor for operations.”

On May 26, 2006, at the University of Kentucky, a faculty member in the School of Human Environmental Sciences had a thumb drive taken from a classroom. The drive may have contained classroom rosters and personal data of students. This is a classic awareness issue for which there is no excuse neglecting in today’s IT security environment.

Table 4-14. My Institution Communicates IT Awareness Issues to Its Faculty, Students, and Staff on a Regular Basis (N = 489)

	Number	Percentage	Cumulative Percentage
Strongly disagree	20	4.1%	4.1%
Disagree	106	21.7%	25.8%
Neutral	124	25.4%	51.1%
Agree	195	39.9%	91.0%
Strongly agree	42	8.6%	99.6%
Don’t know	2	0.4%	100.0%

Table 4-15. Status of Awareness Programs (N = 490)

	Students	Faculty	Staff
Mandatory	17.4%	14.5%	20.4%
Voluntary	37.9%	47.7%	44.4%
No program	44.7%	37.7%	35.2%

Table 4-16. Change in Awareness Programs Offered, 2003 to 2005 (N = 204)

	Students	Faculty	Staff
Program in 2003	39.2%	38.2%	42.2%
Program in 2005	62.3%	68.8%	69.1%
Percentage change	23.1%	30.6%	26.9%

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

It further demonstrates the challenges that central IT faces to secure the overall campus environment.

On average, respondents were neutral about the effectiveness of their IT security programs, with a slightly higher score given to staff awareness programs. Doctoral institutions rated their awareness programs slightly more effective than other Carnegie class institutions. According to Krizi Trivisani, "There are a lot of 'eurekas' when we do training."

Small institutions appear to have special problems. According to John Bruggeman, director of information systems at Hebrew Union College–Jewish Institute of Religion, "When you approach a department or individual about the need to change its business processes to be more secure, they feel like you are chiding them for doing something wrong. You need to convey the feeling that they are not doing anything wrong; the environment has changed. You have to lock the doors in your house now because the neighborhood has changed; you don't live in the country anymore. You can't leave your front door open anymore; you have to make some changes.

My institution still tends to think it lives 'in the country.' Unfortunately, we don't." Our data suggest that such attitudes contribute to the difficulty of establishing awareness programs at the smaller institutions.

Reporting IT Security to Senior Management

We asked how often IT security was discussed at senior management meetings and how often the IT security office made a report to senior management on IT security (see Tables 4-17 and 4-18). We found that 3.7 percent said it was very often discussed at senior management meetings, 20.9 percent said often, 36.8 percent occasionally, 25.4 percent seldom, and 10.4 percent never.

Especially noteworthy is the change in interest by senior management. IT security is increasingly an issue of concern to senior management. The data in Table 4-18 show how reporting to senior management on IT security has increased at the 204 institutions included in both the 2003 and 2005 studies. There has been a sea change in interest in IT security.

Table 4-17. Reporting IT Security to Senior Management (N = 489)

Frequency	Number	Percentage	Cumulative Percentage
Never	51	10.4%	10.4%
Seldom	124	25.4%	35.8%
Occasionally	180	36.8%	72.6%
Often	102	20.9%	93.5%
Very often	18	3.7%	97.1%
Don't know	14	2.9%	100.0%

Table 4-18. Change in Reporting to Management, 2003 to 2005 (N = 204)

Management Reports	Report in 2005	Report in 2003	Percentage Change	Rate of Change
Never	8.8%	14.2%	-5.4%	-38.0%
Seldom	26.0%	34.8%	-8.8%	-25.3%
Occasionally	34.3%	26.0%	8.3%	31.9%
Often	25.0%	14.3%	10.7%	74.8%
Very often	3.4%	2.5%	0.9%	36.0%
Don't know	2.5%	9.4%	-6.9%	-73.4%

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

Reporting on IT security is far more likely at doctoral institutions and least likely at BA institutions. Doctoral institutions (40 percent) report on IT security often or very often, versus an average of 21 percent for other Carnegie class institutions. Similarly, the lower the FTE enrollment, the less likely it is that IT security reports are made to senior management. More than half of the institutions with FTE enrollment below 4,000 reported never or seldom on IT security to senior management.

Budget

Respondents were asked about the percentage of the central IT budget that was dedicated to IT security. The ranges appear in Table 4-19. On average, and regardless of Carnegie class, institutions in our study spend from 1 to 5 percent of their central IT budget

on security. Nineteen percent of the institutions spend 6 or more percent. We also found that institutions with smaller FTE enrollments spend a larger percentage of their overall IT budget on IT security.

The overall change from 2003 to 2005 is minimal, with the exception that far fewer institutions are spending less than 1 percent of their budget on IT security (a one-third change). This is half of the percentage of budget (11.4 percent in North America) reported by *CIO Magazine's* survey of 8,200 IT professionals in 62 countries (see <<http://www2.cio.com/research/surveyreport.cfm?id=93>>).

Future Spending

We then asked about changing expenditure patterns for IT security over the next 12 months. The data appear in Table 4-20. On

average, institutions plan to spend most on security products and training in that order (approximately 10 percent), followed by services and staffing (approximately 5 percent). Doctoral institutions plan to spend the most, especially on training, and BA institutions plan to spend the least, although the differences are minor. Ironically, the institutions that currently spend the most on training are also those that intend to spend even more going forward than those that currently spend the least. These questions were changed significantly from 2003, so comparisons are not possible. A rough reading suggests higher levels of expenditures across the board from 2003.

We asked the respondents whether their institution has provided the needed resources

to address IT security issues, using a Likert scale of 1 to 5 (1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree). The results appear in Figure 4-2. Thirty-nine percent disagreed or strongly disagreed, 27 percent were neutral, and 34 percent agreed or strongly agreed. The numbers are slightly, but only slightly, more positive than those from 2003. And the means are remarkably similar for all Carnegie class institutions, with the exception of MA institutions, which were of the opinion that their resources were less adequate than those of their counterparts. Note also that the projected spending trends mirror the findings of desktoptipeline (see <<http://www.desktoptipeline.com>>).

Lastly, we asked about the institution's

Table 4-19. Percentage of Central IT Budget Spent on IT Security (N = 488)

	Number	Percentage	Cumulative Percentage
Less than 1%	78	16.0%	16.0%
1–5%	253	51.8%	67.8%
6–10%	70	14.3%	82.2%
11–15%	12	2.5%	84.6%
16–20%	8	1.6%	86.3%
Over 20%	3	0.6%	86.9%
Don't know	64	13.1%	100.0%

Table 4-20. Expenditures on IT Security Over the Next 12 Months (N = 490)

	Staffing	Products	Services	Training
Decrease more than 15%	0.2%	0.2%	0.2%	0.2%
–10%	0.6%	1.0%	0.4%	0.6%
–5%	0.2%	0.6%	0.6%	0.6%
0%	55.6%	20.5%	45.3%	26.0%
5%	19.3%	30.4%	25.3%	31.0%
10%	8.2%	27.5%	16.8%	19.4%
15%	4.1%	7.6%	4.8%	9.5%
Increase more than 15%	11.7%	12.2%	6.6%	12.6%

primary justification for IT security expenses. The answers appear in Figure 4-3.

In high-to-low order are strategic investment (25 percent), to meet federal and state compliance requirements (22 percent), incident prevention (20 percent), and reaction to a major incident (14 percent). The compliance factor is the big change from 2003, with the 204

institutions moving from 9.8 percent to 22.0 percent—a change rate of 124 percent. Small colleges more often mentioned reaction to a major incident, whereas doctoral institutions more often mentioned strategic investment. It may be that the ability to secure significant additional funding at small colleges is dependent, in part, on a reaction to a negative event. We

Figure 4-2.
Institution Has Provided Needed Resources for IT Security (N = 490)

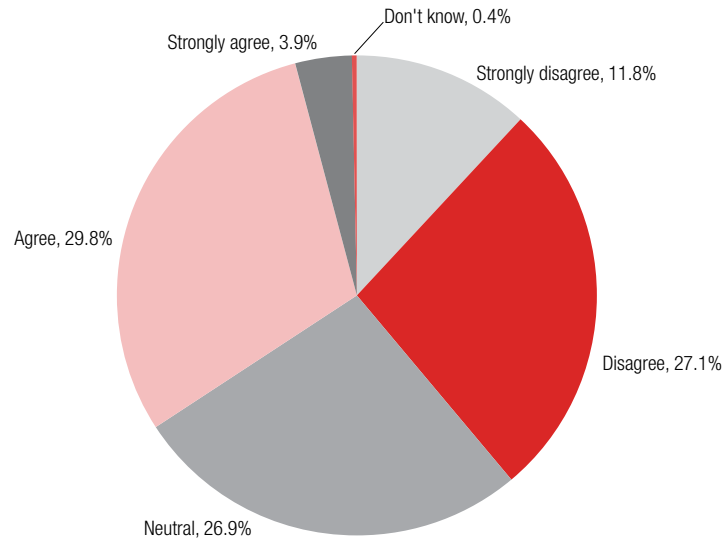
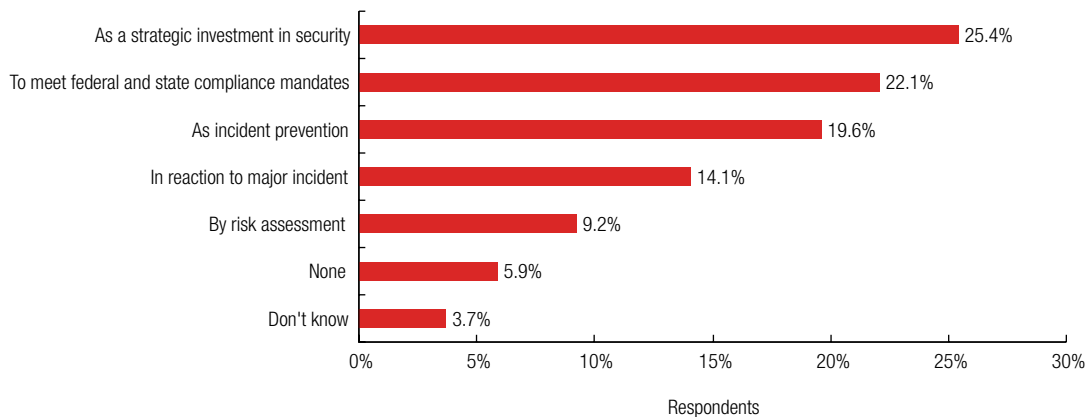


Figure 4-3.
Justification for IT Security Investments (N = 490)



also found that institutions with a dedicated security staff were most likely to justify expenditures as major investments. This may also explain the emphasis on strategic investment we found for doctoral institutions, which more often have a dedicated security staff.

Endnote

1. For an interesting overview of the importance of and interest in certification, see *Worldwide and U.S. security services 2005–2009 forecast* by Allen Carey, at <<http://www.idc.com/getdoc.jsp?containerId=33106>>