

# 5

## Organization, Leadership, Policies, and Awareness

*If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them.*

—Henry David Thoreau

**W**e begin this chapter with the hypothesis that institutions are still in the early stages of establishing an information technology (IT) security culture on campus. IT security is just beginning to gain a foothold in the day-to-day activities that govern an institution's operations.

We also take the position espoused by the Government Accounting Office (GAO) that system security is a holistic problem, in which technological, managerial, organizational, regulatory, economic, and social aspects interact. We discussed technology in Chapter 4. We focus here on the human dimension of security and its foundation.

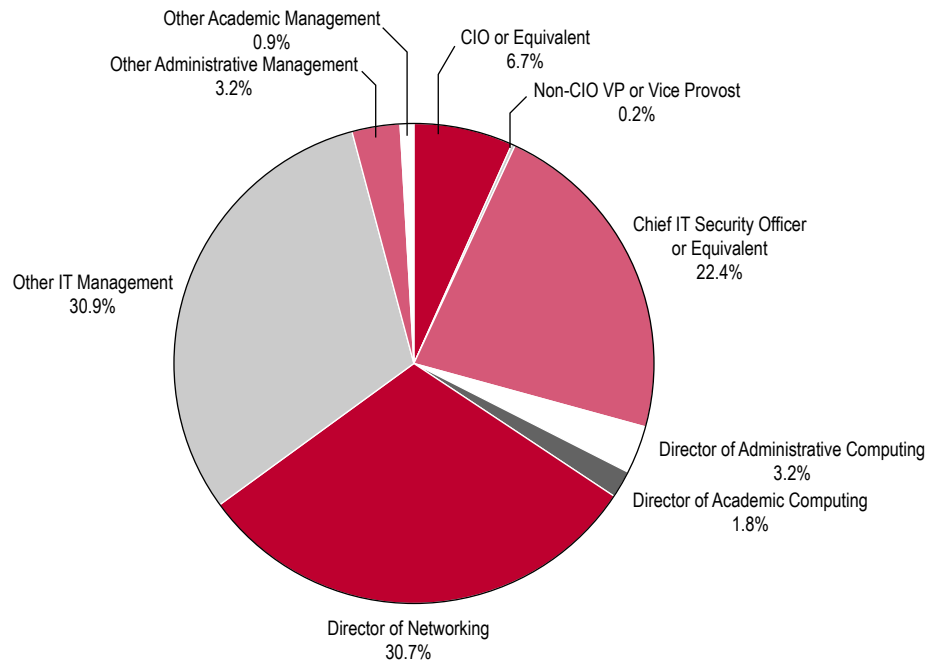
### **Managing IT Security on Campus**

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. The act doesn't specify the person's title, and the job doesn't have to be full time; to whom the position reports is an internal institutional matter. Inevitably, this act will lead most if not all

institutions to designate someone to be in charge of IT security. As a result, the numbers reported in this survey will change shortly. Our survey asked if someone had chief responsibility for IT security. We also asked about their title, when their position was created, their reporting relationships, and what skills and experience they had.

The vast majority of IT security leaders with day-to-day management responsibilities (96 percent) hold their position in the IT organization (see Figure 5-1). Directors of networking are most often in charge (31 percent), followed by chief IT security officers (22 percent) and CIOs (7 percent). The notable differences between Carnegie class institutions are the prominence of IT security officers at doctoral institutions and a greater role for academic management in Canada. Only 20 percent of the U.S. institutions surveyed have a full-time chief IT security officer. In Canada, however, 42 percent of institutions report having a full-time security officer. In the United States, 90 percent of the full-time security officers work at doctoral-extensive and doctoral-intensive institutions.

**Figure 5-1.**  
**Position with**  
**Day-to-Day**  
**Responsibility**  
**for IT Security**



### When Was the IT Security Position Created?

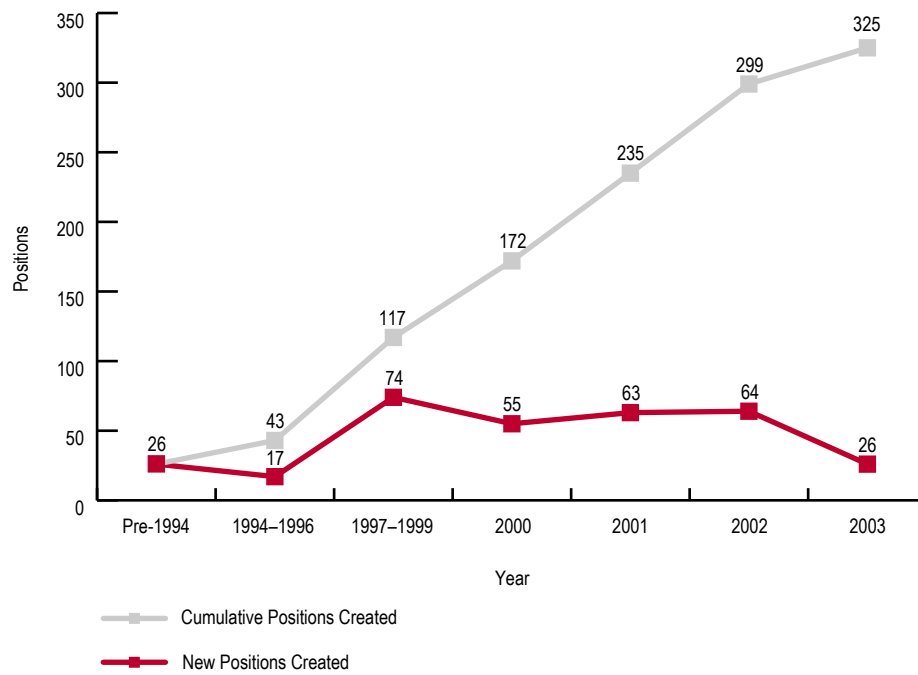
We asked respondents when their institution created the IT security officer position. The results (Figure 5-2) show a clear and steady pattern established in 1994. Canadian, baccalaureate, and master's institutions tended to create the position earlier than doctoral institutions.

Reasons for establishing an office varied. Philip Long, CIO at Yale University, noted that his university established a security office in conjunction with its enterprise resource planning (ERP) implementation. "When we installed our ERP project, it was a logical time to ask about security for a whole set of data that was coming online that hadn't necessarily been online. That was prior to year 2000. We went online in July 1999. We created the security office as an element of our IT system modernization going up to Y2K." South Dakota State University

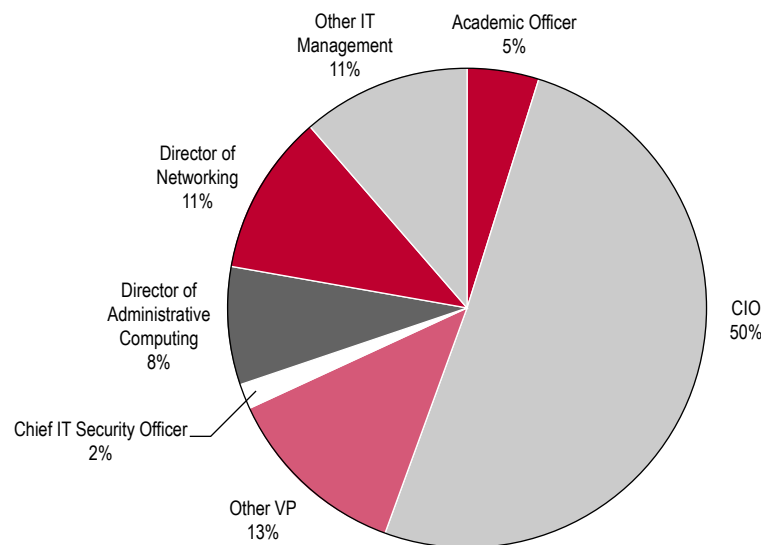
attributed its office in part to government and regulatory issues. At the North Dakota University System, it evolved informally after an outside auditor recommended formal policies and organization for IT security. At the University of Notre Dame, new leadership was a primary factor, as is often the case. For the Maricopa Community Colleges, the September 11, 2001, terrorist attacks were a major factor.

### To Whom Does the IT Security Position Report?

Figure 5-3 shows that fully 95 percent of the IT security officers report to a senior administrator in the IT office, including 50 percent who report to the CIO. Only 5 percent report to academic or other non-IT senior managers. We found minor variations by Carnegie class. Approximately 20 percent of Canadian and associate's institutions report to other non-IT senior managers.



**Figure 5-2.**  
Creation of  
IT Security  
Position,  
by Year



**Figure 5-3.**  
To Whom  
Does the IT  
Security Officer  
Report?

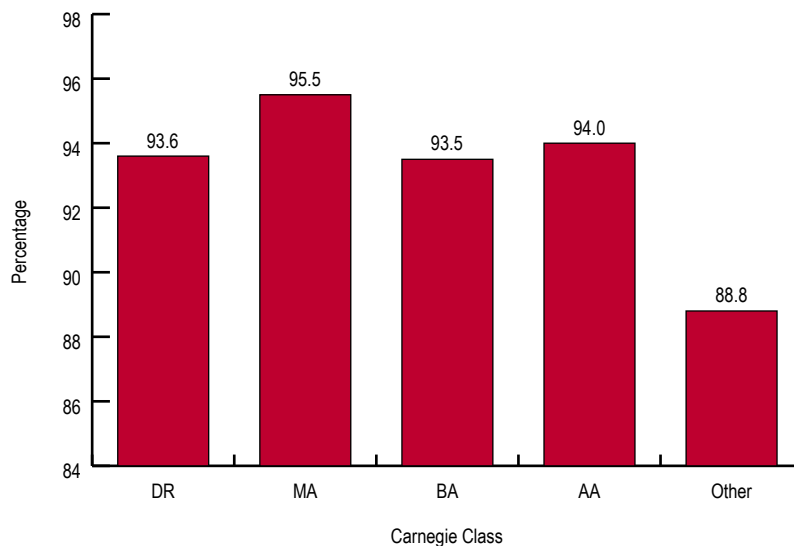
These data are supported by the 2002 EDUCAUSE Core Data Service (CDS) survey, which shows that at 94 percent of 621 institutions, the IT security officer reports to another technology officer (Figure 5-4). Variation by Carnegie class is minimal.

At a CUMREC 2003 panel on IT security, the three panelists—Robert Clark, Jr., director of internal auditing at the Georgia Institute of Technology (Georgia Tech); Derek Kang, corporate compliance director at Shands HealthCare at the University of Florida; and Dan Updegrove, vice president for information technology at The University of Texas at Austin—expressed some difference of opinion regarding where to position the information security officer (ISO) in a higher education institution. Updegrove argued for the ISO's reporting to the CIO: the ISO needs to be independent and partner with deans and others on campus. Kang saw the ISO's reporting to the CIO as a potential conflict of interest, fearing the ISO would filter information, including budget information, given to the president

and other senior managers. Clark thought both were right and said the question is how to create a reporting relationship that operates best on campus. At Georgia Tech, the ISO reports to the CIO, and the CIO and the internal auditor report regularly to the president, the board, and the vice president for finance.

From our in-depth interviews, we learned that Yale University has a dedicated security department with a "dotted-line report" to the auditing department head and a direct report to the CIO. The medical center has a separate organization with full-time security staff. At Indiana University, the Information Technology Policy Office and the Information Technology Security Office report directly to the vice president for information technology. According to Mark Bruhn, chief IT security and policy officer at Indiana University, "Policy and security responsibilities reside in the vice president's office and do not report to the IT department, which signals the importance of keeping them out of areas with direct operational responsibilities."

**Figure 5-4.**  
IT Security  
Officers  
Reporting  
to a  
Technology  
Officer



## Certification

Numerous national security organizations and universities have organized formal IT security training programs that typically award a certificate upon successful completion of a course of study. Twelve percent (54) of the security managers in our survey have IT security certification. Of these, 33 hold the Certified Information Systems Security Professional certificate (CISSP), nine hold the Global Information Assurance Certification, five hold the Earned Security+ certificate, and three hold the Certified Information Systems Auditor certificate. More than half (28) of the recipients are at doctoral institutions. Forty-four institutions report having one staff member with certification, two report having two, three have three, five have four, and one institution reports having more than 10 certified staff members. Again, primarily the doctoral institutions report having certified security staff, although the institution with more than 10 certified staff members is in the Carnegie specialized class.

Andrew Conley, network security officer at South Dakota State University, commented on certification's significance. Having certification is a basis for trust. It shows "we have gone through training and that we have this knowledge. I don't think certification proves knowledge, but it is a qualifier that says you have put in time and the effort. It reassures the user base." Martin Fraser, professor and chair of the computer science department at Georgia State University, agreed. "From the faculty perspective, certification does help—it lends credence and authority that can get the attention of academic units better. [It is] training that is acknowledged."

Gary Dobbins, director of information security, University of Notre Dame, noted

that each of their three security positions is certified. "We wrote that into the position descriptions as a requirement. We value the certification, and it has provided us with a direct benefit on more than one occasion. The certification requirement gave us knowledge in areas we might have otherwise been inclined to pay less attention to."

William Carter, associate vice president for information technology at Austin Community College, gave a mixed review. "One of the problems that I have with certification is that when you finish with the program, your knowledge is out of date. You spend a lot of time taking follow-up courses. Your certification is good for a year afterwards and then your skills are outdated, unless you are using them all of the time. I think experience is more important—day-to-day working on a network is very different from what you learn in a class."

The certification figures for higher education's highest-ranking IT security staff are low, but they mirror some findings for industry. The 2002 KPMG survey found that 73 percent of security staff had no formal security qualifications, 8 percent had earned the CISSP certificate, 5 percent had university-accredited information security qualification, and 7 percent had security vendor certificates. This may be partially attributable to the certification programs' relative newness.

Some campuses also offer their own security training. At Indiana University, for example, the Information Technology Security Office offers a certificate of completion for staff members who complete a series of classes called Security EdCert, specifically designed for local support providers who want to enhance their IT security knowledge.

### Salaries

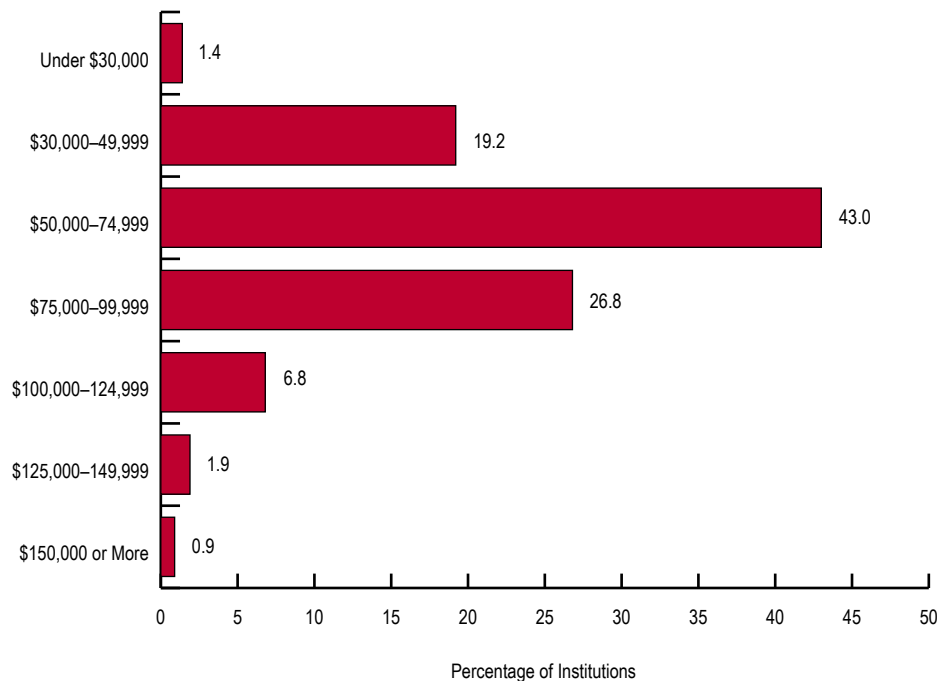
Figure 5-5 shows the IT security position salary range. Forty-three percent are paid in the range of \$50,000–\$74,999; 64 percent earn \$75,000 or less. Salaries are generally higher in private institutions, with the highest salaries almost exclusively reported at doctoral institutions. No salary over \$100,000 was reported in Canada. As we might expect, higher education does not compare favorably with industry here. In a study published by *Information Security* magazine in August 2002, the average salary for a “security manager” across both the public and private sectors was approximately \$121,000, while the average for a “security director” was \$154,000.<sup>1</sup>

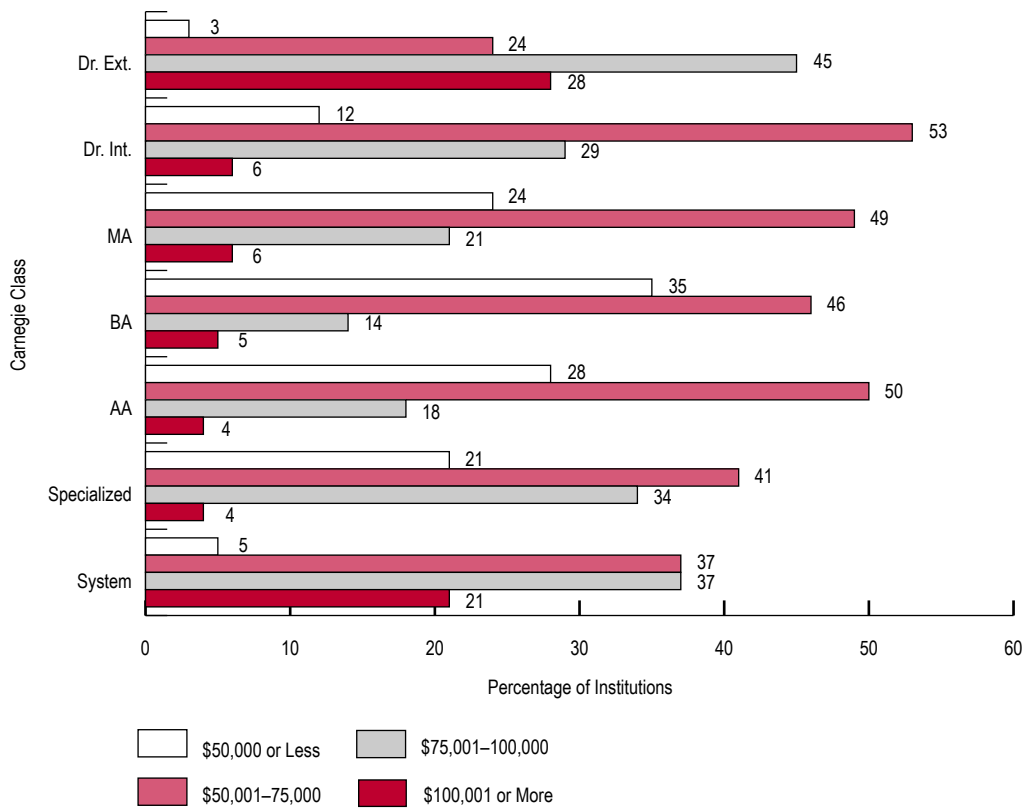
We also looked at whether an institution’s number of networked devices affected salaries, but we found Carnegie class to be a better predictor (see Figure 5-6). For example, security staff at AA institutions with a large number of devices were paid less than staff at doctoral institutions with a similar number of devices.

### Staffing

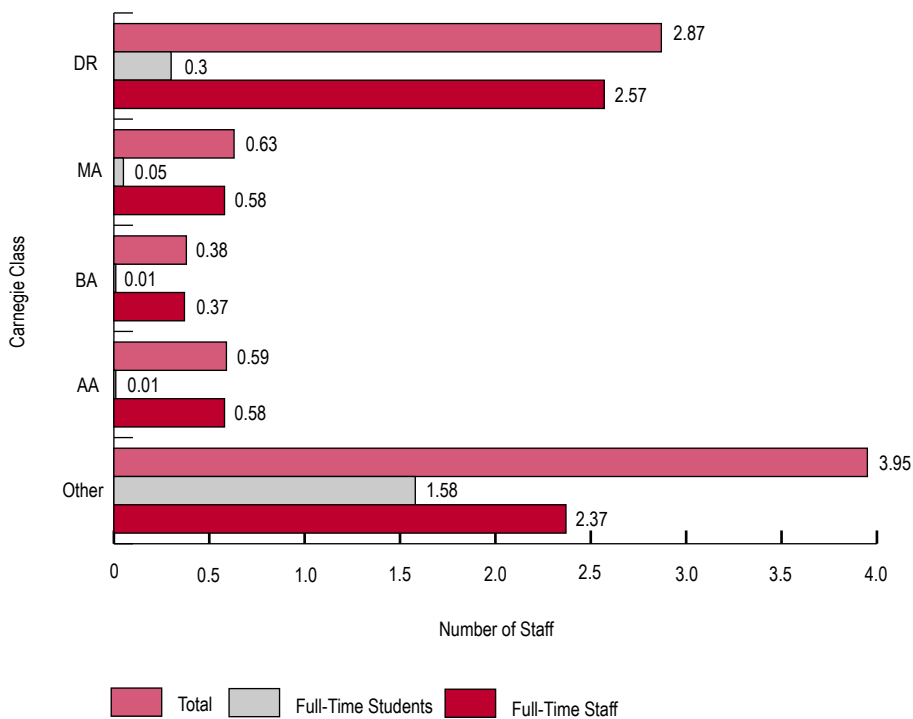
The 2002 EDUCAUSE CDS survey queried respondents on the size of their IT security staff. The mean number of full-time staff and full-time students are provided for each Carnegie class. Clearly the doctoral institutions employ the most IT security staff (see Figure 5-7).

**Figure 5-5.**  
Salary Range  
for IT Security  
Management  
Positions





**Figure 5-6.**  
IT Security Managers' Salary Range, by Carnegie Class and Percentage of Institutions



**Figure 5-7.**  
Full-Time Student and IT Security Staff

The ECAR survey found that 50 percent of the institutions have full-time security staff (see Figure 5-8). Twenty-one percent have one full-time employee managing security, 12 percent have two employees, 3 percent have three employees, and 5 percent have six or more employees. While the doctoral institutions most often have multiple positions, it is interesting to note that every Carnegie class grouping has at least one institution with none, one, or multiple positions.

As the number of networked devices increases, so does the number of full-time staff, especially as the number of devices increases above 10,000. But we still found great variation by size, for reasons captured by The University of Texas at Austin’s Dan Updegrave. “I think it is a very complex model that we would have to develop to determine appropriate IT security staffing levels. You cannot automatically conclude that one campus with 40,000 computers needs twice as many security personnel as another campus with 20,000 computers. The larger campus may have a very uniform IT infrastructure, well-trained users and local system administrators, and locked-down desktops. This reduces the likelihood of problems, so the number of needed security personnel could be comparably modest. The

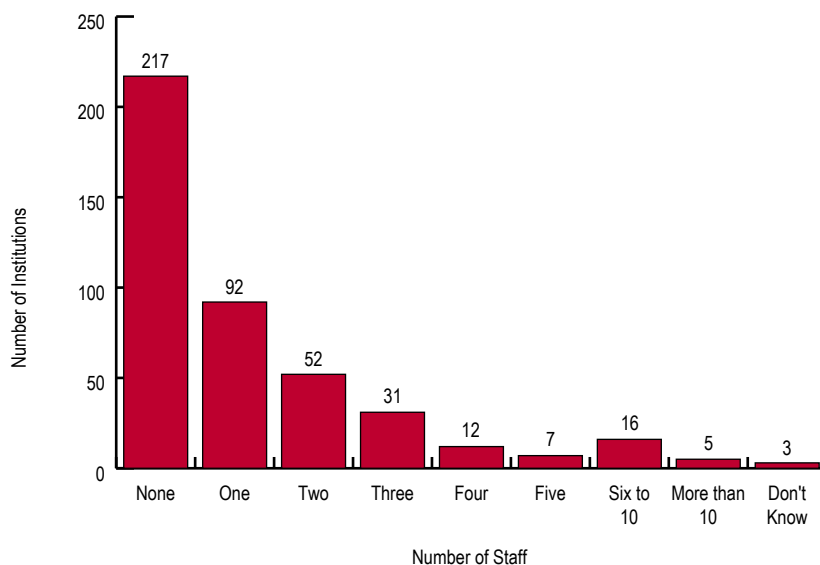
smaller campus may conduct state-of-the-art research, use many domains, have no controls on the desktop, and have poorly trained users. Its exposure may be five times greater than the larger campus. It is extremely hard to get a handle on it.”

The 2002 KPMG survey found the number of full-time-equivalent (FTE) IT security staff to be roughly proportional to organization size, as measured by number of employees. We did not find the same level of proportionality when looking at enrollment and number of users and devices on the network, probably for many of the reasons Updegrave mentioned. But we did find a tendency for the larger institutions to employ more full-time staff.

### Staffing Trends

We asked institutions whether they anticipated changes in the number of IT security employees within the next two years. Fewer than 1 percent (two institutions) indicated a staff decrease, while 66 percent expected no change, 25 percent expected to add one staff member, and 9 percent expected to add two or more. The anticipated increases are largely at doctoral institutions.

**Figure 5-8.**  
**Number of**  
**Full-Time**  
**Central IT**  
**Security Staff**  
**(N = 435)**



Yale's Philip Long provided one interesting perspective on staffing trends. "If I received extra person or budget resources, I would not invest them in IT security. I would invest in critical IT infrastructure, and that helps with security. I don't want more reactive resources; I want more proactive resources, by which I mean building infrastructure so good that the campus can avoid problems."

### Consultants

Outside consultants can supplement institutional staff's efforts and expertise. They provide just-in-time expertise and complementary skills not otherwise available at the institution. Paul Howell, information

systems security officer at the University of Michigan, uses consultants to upgrade firewalls. Otherwise, he says, "I would have to develop an expertise on upgrades. To me it is just cheaper to pay consultants to come in once a year and lead the upgrade effort than to have spare hardware and to devote time and energy to understanding the upgrade process." Many schools have found consultants helpful in explaining the new HIPAA regulations.

Forty-one percent of institutions surveyed had used consultants for IT security-related services in the past 18 months. Of those that had, we asked what services they purchased or were considering. Table 5-1 provides the answers.

**Table 5-1. Security Consultants and Services Used**

Consultant Service	Action (Percentage of Respondents)			
	Purchased	Considered	Did Not Consider	Did Not Use
Managed incident response	1.1	3.4	33.8	61.6
Custom engineering	2.3	4.8	29.9	63.0
Manage projects	3.9	4.4	29.7	62.0
Intrusion detection	3.9	12.6	22.1	61.3
Manage VPN	4.4	5.5	28.7	61.3
Write policy	4.8	10.3	22.3	62.5
Manage antivirus service	5.1	3.7	30.1	61.1
Training and awareness	5.3	9.4	22.8	62.6
Managed firewall	6.4	6.0	26.0	61.6
Physical audit	6.7	9.4	22.3	61.6
Planning	8.3	9.4	21.1	61.0
Technical support	9.0	8.7	20.7	61.6
Architecture/design	9.9	11.0	17.9	60.2
Audit	10.8	10.8	16.3	62.1
Train IT staff	15.9	14.5	7.8	61.8

Clearly, higher education does not extensively use consultants for IT security services. We found their greatest use in training (16 percent), followed by IT security auditing (11 percent), design (10 percent), and technical support (9 percent). With the exception of the largest institutions' hiring consultants slightly more often, we found no noticeable differences in use of consultants or type of service purchased attributable to Carnegie class, institution size, public versus private status, or country.

We asked those who used consultants to evaluate their performance using a five-point

Likert scale: 1 is strongly agree, 2 is agree, 3 is neutral, 4 is disagree, and 5 is strongly disagree. The respondents were for the most part positive (see Table 5-2), expressing strongest agreement on consultants' ability to provide technical expertise (mean of 2.08), product expertise (2.10), and insight from previous projects (2.19). Respondents generally agreed that the consultants helped meet project objectives, get more functionality from the security project, and meet the project timeline. Respondents were neutral on such items as meeting project budget and exceeding expected costs, and were gen-

**Table 5-2. Assessment of IT Security Consultant Services**

Consultant Attribute	Mean	Std. Deviation
Provide technical expertise not available internally	2.08	0.888
Provide product expertise not available internally	2.10	0.909
Brought insight from previous projects	2.19	0.828
Helped to achieve objective	2.29	0.854
Derive more value/function from security program	2.32	0.832
Value for money spent	2.36	0.869
Helped meet project timeline	2.67	0.913
No need for new FTEs	2.77	1.028
Provide project management not available internally	2.98	0.943
Helped meet project budget	2.99	0.849
Cost more than expected	3.10	0.914
Knowledge not transferred to staff	3.18	0.974
Did not understand higher education	3.20	1.033
Experience overstated	3.23	0.997
Personnel not a good fit	3.39	0.839
Did not work well with internal resources	3.56	0.754

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

erally positive on knowledge transfer and ability to work with internal sources. Note that these latter questions were stated in the negative; therefore, the higher mean (three or higher) is the more positive response.

We compared the means and found no noticeable differences attributable to Carnegie class, institution size, public versus private status, or country. Baccalaureate and associate's institutions were slightly more positive about consultants' supplementing internal expertise, which is not surprising because these institutions have, on average, fewer staff than doctoral institutions.

### IT Security Organization

The IT security literature recommends the establishment of a central security office. At an August 2002 NSF workshop in Chicago organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force, participants identified establishing a centralized security organization as the highest priority agenda item in the area of security organization. James Wright, president of Dartmouth College, asserted that "security must be a centralized function, and all functional managers must understand that variance from the campus standard in this area is not an option."<sup>2</sup>

### Advantages of a Central Security Office

The GAO, in its May 1998 *Executive Guide, Information Security Management, Learning from Leading Organizations*, indicated that central security offices can help the institution by

- ◆ serving as catalysts to ensure that information security risks are considered in both planned and ongoing operations;
- ◆ providing advice and expertise to units throughout the institution;
- ◆ keeping top management informed about security-related issues and activities affecting the organization;
- ◆ achieving some efficiency and increasing consistency in the organization's security program implementation by performing tasks centrally that multiple individual business units might otherwise perform;
- ◆ providing training;
- ◆ researching potential threats, vulnerabilities, and control techniques and communicating this information to others in the organization;
- ◆ monitoring 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;
- ◆ establishing a computer incident response capability and, in some cases, serving as members of the emergency response team;
- ◆ assessing risks and identifying needed policies and controls for general support systems, such as organization-wide networks or central data-processing centers;
- ◆ creating standard data classifications and related definitions to facilitate protection of data shared among two or more business units;
- ◆ reviewing and testing the security features in both commercially developed software being considered for use and internally developed software prior to moving it into production; and
- ◆ providing self-assessment tools to business units to let them monitor their own security posture.

Our data confirm the GAO's assertion. Institutions with a dedicated security staff will much more likely fulfill the above functions.

## Centralized and Decentralized Security Offices

Our interview data provided examples of organizational structures. Indiana University (IU) established two distinct offices: the Information Technology Policy Office (ITPO) and the Information Technology Security Office (ITSO). These offices are intentionally distinct: the ITPO handles IT policy development, dissemination, and education, and the ITSO handles security analysis, development, education, and guidance for IU's information assets and IT environment.

While not splitting security into distinct offices, several institutions we interviewed already segment, or plan to segment, functions within the security organization to focus on either technology versus policy or academic versus administrative security issues. For example, South Dakota State University plans to split their chief security officer position into two, one with a technical focus and the other with a culture interface/awareness focus. Yale University has two functional areas in their security office: one technician focuses on administrative security issues and the other on academic security issues.

The quantitative data in Figure 5-9 reflect that 57 percent of institutions spread IT security across multiple functional areas; only 11 percent have a dedicated IT security staff. At 22 percent of the institutions, IT security is the responsibility of a single individual. Two institutions outsourced their IT security.

As Figure 5-10 illustrates, we found 50 percent of the dedicated IT security staff offices at doctoral institutions and 90 percent at doctoral, system, and specialized institutions (notably medical schools).

## Security Policy

According to the GAO, "The framework within which an organization strives to meet its needs for information security is codi-

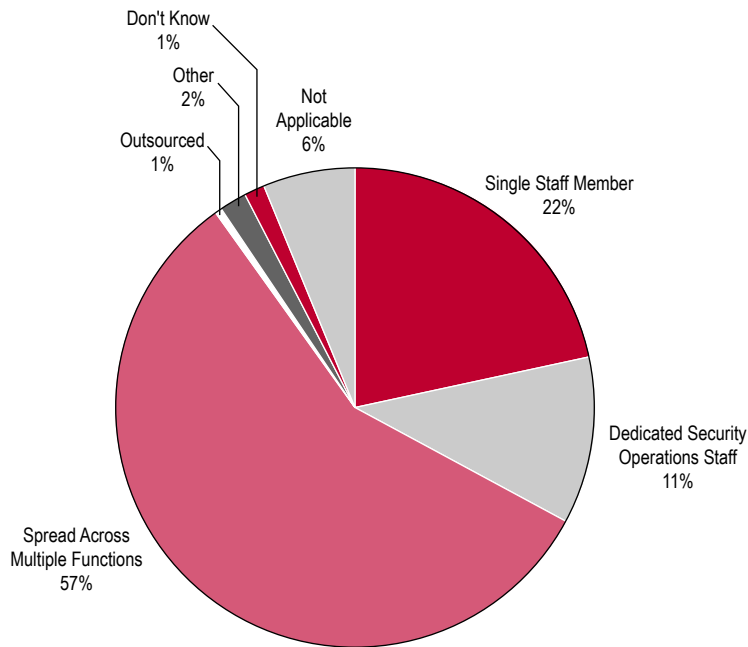
fied as security policy. A security policy is a concise statement, by those responsible for a system (such as senior management), of information values, protection responsibilities, and organizational commitment."<sup>3</sup>

Scott Blake of BindView Corp. and Patrick McBride of the META Security Group stated that a security policy provides a framework for

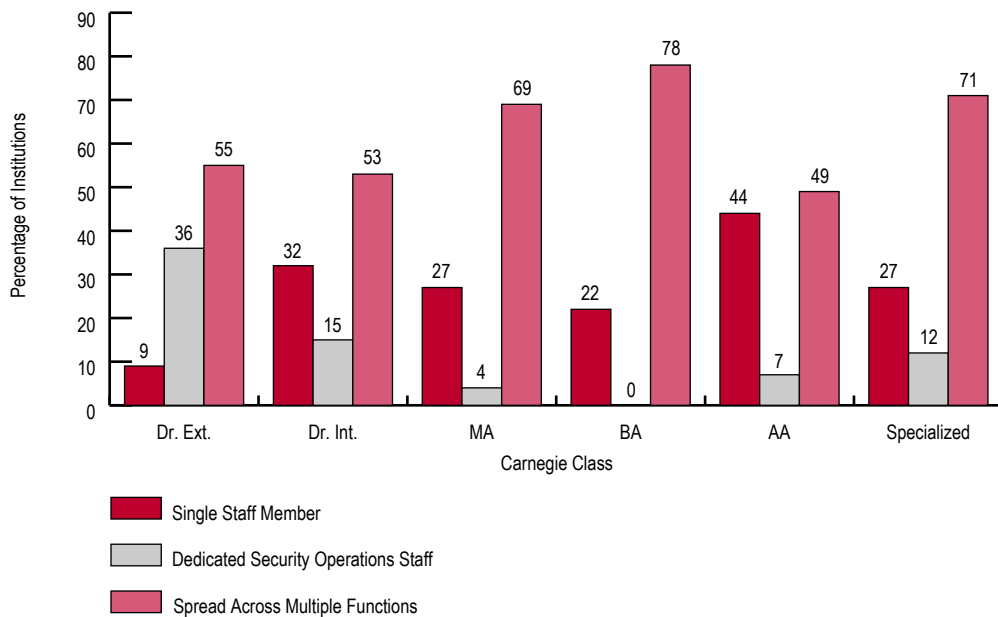
- ◆ making consistent, timely, and cost-effective management decisions;
- ◆ selecting security controls and products;
- ◆ defining and empowering acceptable behavior [by students, faculty, and staff]; and
- ◆ empowering [members of the institution's community to do their work] securely.<sup>4</sup>

A security policy can also establish goals. Gordon Wishon, CIO of the University of Notre Dame, said, "The primary goals at this time are, one, to address liability for the university—legal and civil liability that results from a mishandling and/or misappropriation of protected information; two, a secondary but almost equal concern is the effort, energy, cost, and expense of dealing with incidents and clean up from viruses; and three, the concern that we have for students and faculty and protecting them from some of the negative effects of life on the Internet."

Indiana University's Mark Bruhn explained, "Institutional values drive policy; policy dictates processes, procedures, and standards; and security implements those." We would elaborate on Bruhn's astute observation. Several IT security commentators have expressed concern that IT security can be inimical to academic freedom, but we believe this depends on the policy driving IT security at a particular institution and not on the tools themselves. Indeed, IT security can support academic freedom by ensuring



**Figure 5-9.**  
Operational Staffing Structure for IT Security (N = 435)



**Figure 5-10.**  
Operational Staffing Structure for IT Security, by Carnegie Class (N = 413)

ready and timely access to information by authorized users. This is a major reason for having a comprehensive IT security policy: it can embed the academy's most important values into an area that some might otherwise find problematic. We elaborate on this topic in Chapter 10.

Moreover, IT security policy is critical to holding all parties in the institution accountable. As Blake and McBride point out, "Because security measures are disaster-preventing rather than payoff-producing, a central aspect of security must be accountability. That is, users and operators must be

held responsible by management for taking all appropriate security measures. One cannot count on financial and market incentives alone to drive appropriate action. Many security problems exist not because a fix is unknown, but because some responsible party has not implemented a known fix."<sup>5</sup> A good security policy can play an important role in liability abatement by demonstrating that the institution has taken appropriate and necessary precautions to protect its information assets and clients.

### Campus Policies

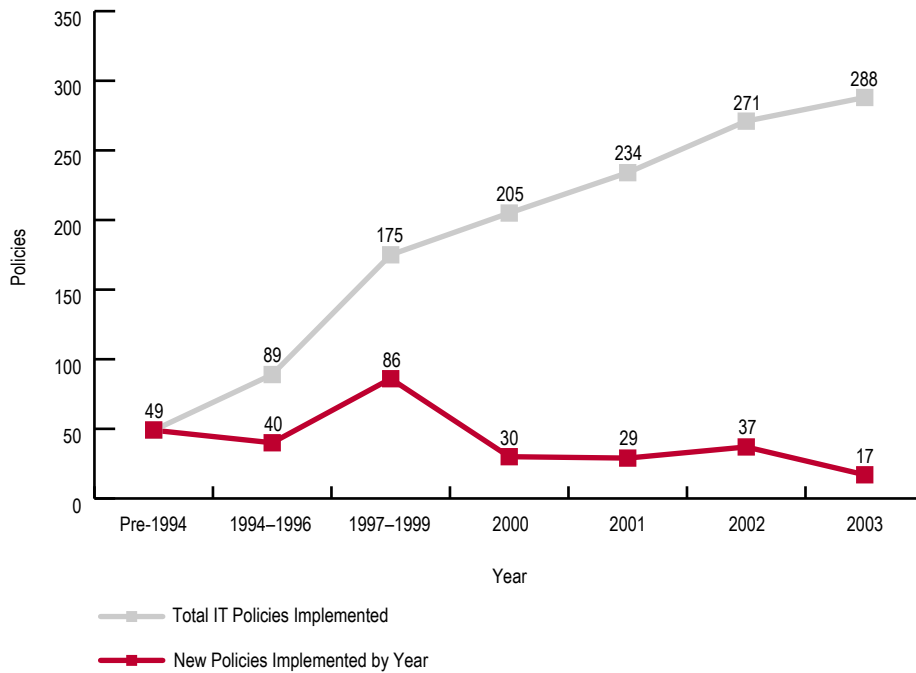
Where and when have security policies been implemented? Who was involved in their development? What policies have institutions put into place regarding access to and usage of their networks, computing resources, applications, and data or information resources? Are these policies enforced and updated? What reactions, if any, did these policies generate on campus? What emerging issues are forcing policy changes? How are institutions reacting?

Fifty-four percent (235) of the institutions queried indicated that they have a formal institutional policy (or policies) covering IT security (see Table 5-3). Nineteen percent of the 235 institutions with formal policies also had interim policies or were implementing additional policies. Twenty-three percent of respondents had no formal policy but did have an interim policy; an additional 15 percent were implementing a formal policy. Only 8 percent had no policy, formal or interim.

Figure 5-11 shows that institutions are steadily putting in place formal IT policies. Table 5-4 indicates which security areas the formal policies cover for all institutions and by Carnegie class. Virtually all policies address appropriate use of institutional assets, and 80 to 90 percent of policies cover system access control, authority to shut off Internet access, data security, network security, enforcement of institutional policies, and desktop security. Policies less often address physical security of assets, residence halls, remote devices, and application development

**Table 5-3. IT Security Policies in Place**

Status of Policies	Number of Institutions	Percentage
Implemented, interim, and implementing	45	10.3
Implemented and interim policies, not implementing	13	2.9
Implemented, no interim, implementing	24	5.5
Implemented, no interim, not implementing	153	35.2
No formal policy, have interim, are implementing	39	9.0
No formal policy, have interim, not implementing	62	13.7
No formal policy, no interim, are implementing	64	14.7
No formal policy, no interim, not implementing	35	8.0



**Figure 5-11.**  
Year IT Security Policies Were Implemented

**Table 5-4. What Do the Policies Cover? Differences by Carnegie Class and Canada**

What Formal Policies Cover	Positive Response, by Carnegie Class (Percentage of Respondents)								
	All	Dr. Ext.	Dr. Int.	MA	BA	AA	Specialized	System	Canada
Appropriate use of institutional assets	99	99	97	99	99	100	90	94	100
System access control	89	83	91	90	90	88	88	71	79
Authority to shut off Internet access	85	89	89	80	90	67	81	82	84
Data security	83	80	86	79	86	84	78	71	68
Network security	82	78	86	84	83	79	82	71	79
Enforcement of institutional policies	82	75	88	78	80	86	81	65	79
Desktop security	80	70	71	72	91	88	86	52	74
Physical security of assets	71	62	66	67	71	72	76	65	68
Residence halls	61	75	74	68	70	7	42	44	53
Remote devices	51	51	54	42	51	45	52	41	53
Application development	39	32	40	41	31	35	38	41	29

policies, but note that at many institutions included in the study, residence halls and remote devices are not available and application development is not undertaken.

We found some differences among Carnegie classes. Doctoral-intensive and baccalaureate institutional policies are more likely to exceed the average coverage for all areas, and doctoral-extensive and Canadian policies are less likely to exceed the average. Small institutions' policies more likely exceed the average on desktop security. There was very little difference between private and public institutions, with the exception of application development (41 percent "yes" at public institutions and 29 percent "yes" at private institutions). Private institutions' policies were more likely to cover residence halls (72 percent versus 51 percent for public), but that may be attributable to the very low number of residence facilities at AA institutions (only 8 percent have residence halls), which are mostly public (48 of 51) in this study.

Specificity varies, too. The North Dakota University System segments their security policies into five areas: network security, data security, desktop security, physical security,

and system security. Philip Long, CIO, said Yale University has "an overall appropriate use policy that makes it clear that anything that threatens the network is prohibited and that any misbehaving machine will be disconnected. We do not have a policy that goes into detail—you may not run a machine that is compromised with a virus, etc. Rather we have general language that any IT action that is impeding the community is prohibited. Then, we use, in theory, good judgment."

### Security Policy Characteristics

Security policies must be easy to read, accessible, enforced, comprehensive in scope, regularly updated, and consistent across the institution. We asked respondents to assess their institution's IT security policies on each of these dimensions. Table 5-5 shows the mean value and standard deviation for each characteristic in rank order. The mean is based on a four-point Likert scale: 1 is strongly agree, 2 agree, 3 disagree, and 4 strongly disagree.

There is stronger disagreement about policies being regularly updated and comprehensive. A few institutions men-

**Table 5-5. IT Security Policy Characteristics**

Policy Characteristic	Mean	Std. Deviation
Policies are accessible	1.92	0.708
Policies are clear and easy to read	1.98	0.583
Policies are consistent across the institution	2.08	0.748
Policies are enforced	2.09	0.659
Policies are regularly updated	2.44	0.717
Policies are comprehensive	2.53	0.798

Scale = 1 (Strongly Agree) to 4 (Strongly Disagree)

tioned that they avoided updating policies because of an arduous approval process. Our respondents ranked the characteristics “accessibility” and “easy to read” highest among the six characteristics. We also looked for differences between public and private institutions and between Carnegie classes, as well as differences by institution size. Respondents from private institutions ranked all policy characteristics more favorably than did those from public institutions, but only by a very small amount. Otherwise, differences were minor and not significant.

Indiana University emphasized the need for easy-to-understand security policies. “Policies must be easy to read, understand, and interpret,” emphasized Merri Beth Lavagnino, deputy IT policy officer. “Even though we have foundation policies, it’s very difficult for the person who doesn’t work with them every day to understand them. These folks call Mark [Bruhn] or me. We need to work on education and awareness. I’d love to spend more time in making policies more accessible—maybe have an ‘ask the policy guy.’” Bruhn agreed. “We need and want the formal policies to exist, but also need another format that makes them easier to read, less formal, and more narrative.”

### **Leadership’s Involvement in Policy Development**

The best-practice literature on policy development encourages senior management’s active engagement, not simply their support or endorsement. Dartmouth College President James Wright said, “Privacy and academic freedom are critical components of campus culture; it is vital that decisions on policies and practices regarding security and related issues be carefully vetted, understood, and authorized by both the highest levels of the campus leadership and the

representatives of the campus community. The executive role in all of these matters is crucial if internal dissention and unnecessary strife are to be avoided.”<sup>6</sup>

Georgia Tech’s Robert Clark, Jr. advised attendees at the CUMREC 2003 Security Panel, “If you’re asked to develop policies, don’t do it on your own. It is a shared responsibility. At Georgia Tech we have a committee with legal, audit, vice president for human resources, vice president for finance, an assistant dean, student, CIO, and director of information security. First do an evaluation and assessment of risk. Assess the degree of risk at the institutional level. Often the risk is being assumed by default rather than thinking about it—it is not up to the individual units to decide. Raise the visibility of security so that the president makes the decision.”

When Michael McRobbie, Indiana University’s vice president for information technology and CIO, came to IU in January 1997, he immediately established a good working relationship with then-president Myles Brand. Brand became a strong advocate for IU’s security efforts. This executive-level support enabled IU to proceed more quickly in adopting security policies and practices than it could have without this support. Because IT security is very much a cultural issue, the leaders who can most effectively change the institution’s culture must be visible and engaged.

Also important for changing the culture are the governance groups. In a May 2003 presentation to the Common Systems Group, Jack McCredie, CIO of the University of California, Berkeley, recommended, “The policy development process should include engaging the IT governance structure for collaboration and policy formulation, providing opportunity for input throughout the development process, soliciting

input from non-IT committees, obtaining approvals from senior management, and communicating, communicating, communicating.”

James Wright of Dartmouth suggested that “with security issues, the parties that may need to be involved are potentially quite different from those that were involved in past years.”<sup>7</sup> IT security impinges on ethical and philosophical issues, on teaching and research as well as on most business areas, and it goes beyond a single college or unit.

### Data on Leadership Involvement

We asked our respondents about their senior management’s level of involvement in developing their institution’s security policies (see Table 5-6). We calculated the mean and standard deviation for each administrator, office, or agency on the basis of a five-point Likert scale.

We found the most agreement and the least difference of opinion on the active engagement of the IT organization and the CIO. Senior academic officers, the board, and external state agencies are not seen as having anywhere near as much involvement in IT security policy development.

We also looked for differences based on public versus private institution, institutional size, and Carnegie class. Overall, we found few differences and nothing of statistical significance. Those at private institutions see the board and president as less involved than do respondents at public institutions. Senior administrators other than the CIO are seen as more involved at AA institutions, probably because there are fewer CIOs at these institutions. The faculty and internal auditor were more engaged at doctoral and larger institutions. And Canadian institutions mirrored their American counterparts across the board.

**Table 5-6. Participants in the Development of IT Security Policy, Ranked by Level of Participation**

Participation	Mean	Std. Deviation
IT Organization	1.74	0.726
CIO	2.06	0.977
Campus/Faculty Task Force	2.89	1.262
System Office	3.10	1.245
Internal Auditor	3.31	1.149
Provost	3.48	1.160
External Auditor	3.58	1.094
President	3.67	1.035
Board of Trustees	3.90	0.927
State Agency	4.03	1.012

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

## The Leadership Challenge

Our data suggest that a concern for IT security has not been adequately carried forward to the executive level. An executive vice president of a large research university confirmed this view when asked about his level of involvement with IT security. He replied, "That is mostly left to the technology folks and to the CIO, at the vice president level. Most other executives aren't deeply involved, except at the medical center."

One reason for their lack of interest may be that historically, IT security breaches, when they have occurred, haven't impacted the institution, or the executives themselves, as much as other incident types. For example, we found no documented instances of a university executive losing his or her job over an IT security breach, whereas incidents such as financial fraud and athletics scandals have brought down university administrations.

## Awareness

Is the campus community well educated about security risks? Are awareness programs and practices in place, if so for whom, and are they effective? The issue is critical, as many believe that the greatest risk to the institution 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 their password to someone over the phone. The 2003 Healthcare Information and Management Systems Society Leadership Survey indicated that an internal security breach was the primary threat to their organizations (55 percent of the respondents). External threats scored 23 percent. Gregory Jackson, vice president and CIO at the University of Chicago, said his "biggest concern is that a very large portion of the people who connect to the network

have no concept of security and [are] showing up with improper setups."

Continuous security education is likely one of the most cost-effective and important defensive strategies an institution can take, and several helpful Web sites offer good ideas.<sup>8</sup> At the NSF Security Architecture and Policy Workshop in August of 2002 in Chicago, attendees asked to rate priorities for an action agenda cast the most votes (34) for a campus-wide security awareness campaign. They also highly supported sharing training materials across campuses (21 votes), developing security training and education courses for staff and faculty (20 votes), and building awareness among higher education executives regarding security issues and risks (16 votes). Notre Dame's Gordon Wishon noted the importance of awareness: "The lack of attention to security is a long-standing situation and has led to a huge awareness gap. We should invest in a very high degree of awareness. Awareness building does not have to cost a lot of money, but it definitely needs attention." Our data show the priority is a pressing one, as awareness programs on many campuses are not as strong as Wishon and the authors believe they should be.

Kim Milford, information security manager at the University of Wisconsin–Madison, emphasized the importance of building campus security awareness. "One important area of awareness that we've developed is an annual security conference, called Lock-down," she said. "UW–Madison system administrators, IT staff from other University of Wisconsin institutions, and IT staff from state agencies attended this two-day conference. We bring in regional and national speakers to discuss current security issues, such as legal considerations, risk assessment, and Microsoft security. The content includes both technical and policy topics. It provides a great opportunity to get campus

system administrators together to discuss security as well as increase their education and awareness.”

### IT Security As a Campus Priority

We asked the respondents whether IT security was one of the top three issues confronting their institution today. Seventy-five percent agreed or strongly agreed that it was, 15 percent were neutral, and 10 percent disagreed or strongly disagreed. Respondents who strongly agreed were most likely to come from large doctoral institutions. We also asked whether IT security was a priority of their institution. Sixty-one percent agreed or strongly agreed that it was, 25 percent were neutral, and 14 percent disagreed or strongly disagreed. The mean on a scale of 1 to 5 (1 is strongly agree, 2 agree, 3 neutral, 4 disagree, and 5 strongly disagree) was 2.39. Again, respondents who strongly agreed were most likely to come from large doctoral institutions.

### Reporting

We asked how often IT security was discussed at the president’s or chancellor’s cabinet meetings and how often the IT security office made a report to senior management on IT security. Fewer than 1 percent said it was very often discussed at cabinet meetings, 10 percent said often, 29 percent occasionally, 29 percent seldom, and 9 percent never. One-quarter of the respondents answered “don’t know.” For reporting, the percentages were higher, with 3 percent saying very often, 14 percent often, 37 percent occasionally, 31 percent seldom, and 15 percent never. Eight percent did not know. Institutions reporting “never” were most often small, with 2,000 or fewer enrolled students.

Table 5-7 shows the periodicity of reporting to senior management, by Carnegie class. We found reporting to be more likely at doctoral institutions. However, in light of best practices, these numbers are low. Not surprisingly, for institutions that had an

**Table 5-7. IT Security Reporting to Senior Management, by Carnegie Class**

Carnegie Class	Reports to Senior Management (Percentage of Respondents)				
	Very Often	Often	Occasionally	Seldom	Never
Dr. Ext.	2.7	20.3	43.2	27.0	6.8
Dr. Int.	–	19.4	41.9	25.8	12.9
MA	4.0	10.9	34.7	32.7	17.8
BA	1.3	13.9	20.3	43.0	21.5
AA	2.3	11.6	39.5	30.2	16.3
Specialized	2.0	6.0	46.0	24.0	22.0
System	6.7	13.3	60.0	6.7	13.3

incident reported in the press, the reporting level was higher.

We did a means comparison on reporting and looked at Carnegie class (Table 5-8). The lower the mean, the more often reports were made to senior management (1 is very often and 5 is never).

The number of devices proved to be the better predictor. The more devices on the network, the more often reports were made (see Table 5-9).

Indiana University's president and board of trustees have clearly made IT security a priority. Through regular briefings and discus-

**Table 5-8. Mean Frequency Reporting to Senior Management by Carnegie Class**

Carnegie Class	Mean	N	Std. Deviation
Dr. Ext.	3.15	74	0.917
Dr. Int.	3.32	31	0.945
MA	3.50	101	1.036
BA	3.70	79	1.005
AA	3.47	43	0.984
Specialized	3.58	50	0.971
System	3.07	15	1.033
Total	3.45	393	0.999

Scale = 1 (Very Often) to 5 (Never)

**Table 5-9. Reporting to Management by Number of Network Devices**

Number of Devices	Mean	N	Std. Deviation
Under 1,000	3.63	64	0.864
1,001–5,000	3.56	168	1.031
5,001–10,000	3.63	67	0.967
10,001–20,000	3.00	45	1.044
20,001–40,000	3.10	21	0.889
40,001–60,000	3.17	12	0.835
60,001–80,000	2.60	5	0.548
More than 80,000	2.50	4	0.577
Not Centrally Tracked	3.00	6	0.894
Total	3.45	392	1.000

Scale = 1 (Very Often) to 5 (Never)

sions with McRobbie, the board has come to understand the risks to the institution of poor security. After a security breach resulting in the release of personal information from the Office of the Bursar in early 2001, the board voted to quantify and strengthen the vice president of information technology and CIO's responsibility with a resolution that the office assume leadership, responsibility, and control of responses to unauthorized access to IU's IT infrastructure.

We asked respondents if IT security practices were woven into the institution's business practices. The majority (58 percent) were neutral or negative. On a Likert scale of 1 to 5, the mean value for the respondents was 2.89. Doctoral-intensive institutions did best, but on the whole we found little difference among institutions of varying size or Carnegie class, and between public versus private or United States versus Canada.

We did see more variation when asking whether "IT security problems inadvertently caused by authorized users are significant." A majority agreed or strongly agreed that this was a problem. On a Likert scale of 1 to 5, the mean value for the respondents was 2.59, which suggests a fairly even divide. Larger schools and doctoral institutions were more likely to see it as a problem. The University of Texas at Austin provides a good example: the SQL Slammer worm was under control until an MBA student came to campus and plugged in an infected laptop inside the firewall. Clearly, it is a challenge for the ordinary user to learn about ports, time limits, advisories, and so on.

The dilemma here is that people take security for granted. We know that many deans or directors provide their personal assistants with their user IDs and passwords for

reading their e-mail. Such behavior, while understandable at one level, nevertheless suggests a serious vulnerability to their other personal information and access privileges. Awareness programs are key to improving IT security behavior.

## Awareness Programs

Surprisingly, only one-third of the institutions had a formal awareness program for students and faculty (see Figure 5-12). Only slightly more—39 percent—had a formal awareness program for staff. Again, we found some differences by Carnegie class: doctoral institutions were more likely to have awareness programs. We found no differences between public versus private or Canadian versus American institutions.

Doctoral institutions, which are more likely to have a dedicated IT security staff, are also therefore more likely to have formal awareness programs (Figure 5-13). Also, the larger the dedicated IT security staff, the more likely there will be a formal awareness program.

Numerous institutions have developed security awareness programs as part of student orientation. At Embry-Riddle Aeronautical University, for example, a formal training program for students called Back to School explains to students and their parents their rights and responsibilities. Students go through a half-hour program during orientation before they receive their PINs and passwords.

Doug Kankel, professor of molecular, cellular, and developmental biology at Yale University, evaluated the level of faculty awareness: "I would say that faculty-wide awareness is not high. The awareness level probably scales in some way with the so-

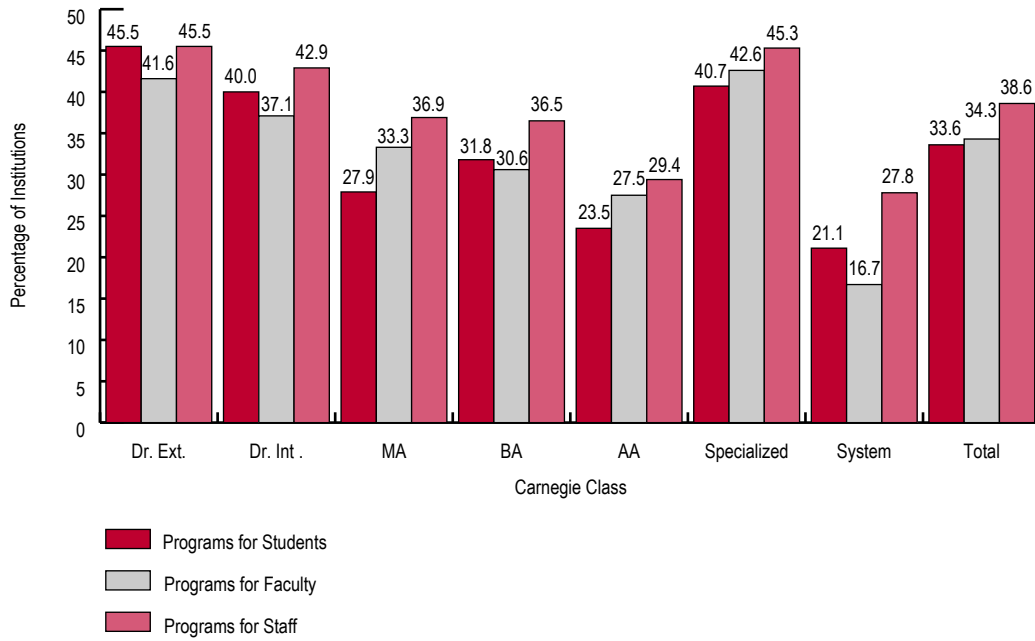


Figure 5-12. Awareness Programs, by Carnegie Class

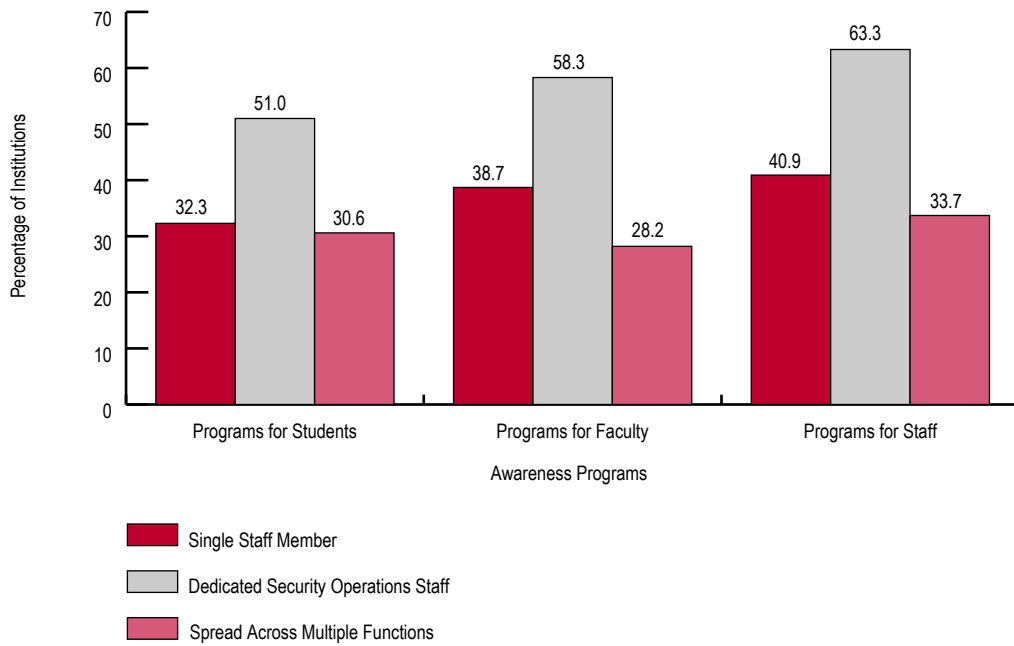


Figure 5-13. Awareness Programs, by Type of IT Security Organization

phistication of the user and the specific demand. People who are running servers that are in fact reaching a larger set of individuals are probably more aware than individuals that are simply using a personal machine attached to the campus network. The further away one is from more sophisticated computing, the less one is aware of what the issues are."

Creativity is also important to building security awareness on campus. "We've gone beyond just using Web announcements, newsletters, and e-mail—we're creative with our awareness efforts, using such mediums as radio ads, videos, posters, and even putting messages on campus ATM machines," said University of Wisconsin–Madison's Kim Milford. "Often the statistics from our incident response team feed into our awareness efforts. The areas of largest concentration of incidents, such as copyright infringement, become the areas in which we focus our awareness efforts. We also get students to assist in developing our awareness programs, such as student creation of security videos. We find they understand the student audience better than we do."

*Information Week's* 2002 Global Information Security Survey indicates that only 27 percent of U.S. companies have conducted security training. Our data show slightly better performance by higher education. The percentages are disappointing, as this is one area where increased expenditure and effort could have an enormous payback to the institution. Security is much more than firewalls and antivirus tools. It is not obtained simply through the purchase of new technologies.

### **Effectiveness of Awareness Programs**

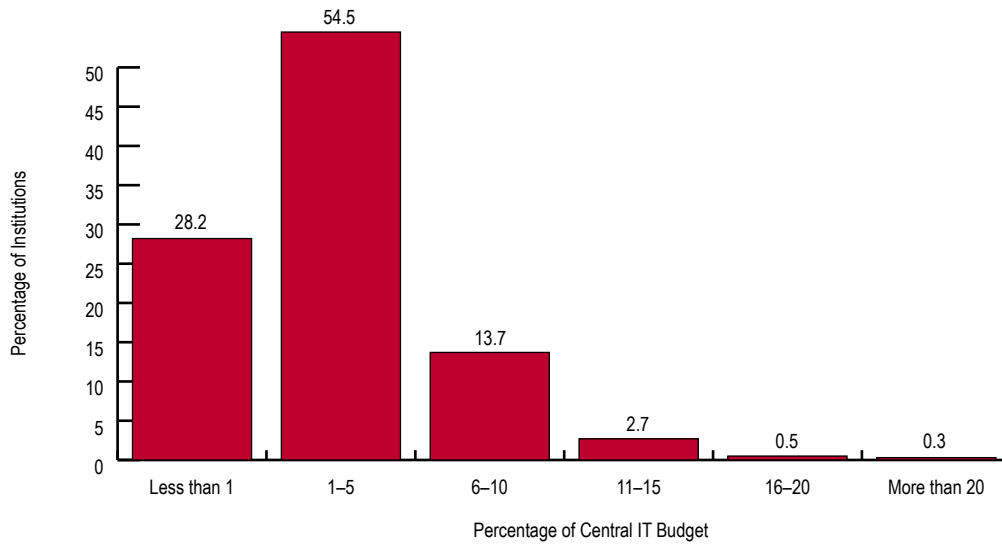
When asked how effective the respondents felt their awareness programs had been, 70 percent were neutral or negative

about the programs for their students and faculty (mean of 2.97 for students and 2.93 for faculty on a scale of 1 to 5, where 1 is strongly agree and 5 is strongly disagree), and 60 percent were neutral or negative for staff (mean of 3.78). There was little difference based on institution size, Carnegie class, public versus private status, or Canada versus the United States.

Andrew Conley of South Dakota State University provided a typical assessment of an institution's awareness programs: "I'd say that the majority of faculty and staff are not aware of the policies, even though they are published on the Web. Some actions we are contemplating include a banner that pops up whenever a user logs in to a computer, stating that he or she agrees to the acceptable use policy and pointing the user to a site to view the policy. And also, we want to create a Web site and make everyone visit it and sign off with some sort of digital signature saying that they have agreed to it. The students are probably more aware of policies than the faculty because they have a small, short executive summary of the policy that they have to sign before they get Internet access."

### **Budget**

We asked respondents about the percentage of the central IT budget dedicated to IT security, and we present the range and answers in Figure 5-14. Of the respondents who provided data for this question, 55 percent spent from 1 to 5 percent of their central IT budget on security, and 14 percent spent 6 to 10 percent. Twenty-eight percent spent less than 1 percent. The 2002 EDUCAUSE CDS survey found that, on average, 86 percent of IT security funds came from the operating budget, 6 percent from the capital budget, and, at doctoral institutions, 10 percent from indirect cost recovery.



**Figure 5-14.**  
**Percentage**  
**of Central IT**  
**Budget Spent**  
**on IT Security**

We had anticipated that the larger the institution, the smaller the percentage of its budget that would be spent on IT security. That is the reported case for private industry (*Information Week's* 2002 Global Information Security Survey). *Information Security* magazine's 2002 survey of 2,196 IT security practitioners showed that the larger the organization, the less it spends on security per user and per device. But we found no differences in the percentage of budget support among institutions of varying size, Carnegie class, public versus private status, or United States versus Canada. *Information Security* magazine's survey estimated that education spends about 4 percent of the IT budget for security, which is very close to our findings. These comparison figures might be misleading because many higher education institutions may spend a significant amount

of money on IT security outside of the central IT organization, which would make the comparison numbers more favorable.

Universities spend less on security than government, banking, telecommunications, and other industries reportedly spend. According to *Information Week's* 2002 Global Information Security Survey, fielded by PricewaterhouseCoopers, businesses spend on average 12.4 percent of their overall IT budget on IT security. The same survey indicated that education spent about 10 percent, but our numbers do not corroborate their findings. KPMG asked businesses how much of the IT budget was spent on security last year and whether it will be increased or decreased next year. They found that the average spent on IT security was USD\$2.6 million, an average of 10.1 percent of the IT budget.

### Future Spending

We then asked about changing expenditure patterns for IT security over the next 12 months. Table 5-10 presents the data.

Respondents expected training and hardware and software expenditures to increase more than staffing and external services, which almost two-thirds of the respondents thought would stay the same. Although they saw no difference for external services, the large-enrollment and doctoral institutions expected some increases in expenditures for staffing, training, and hardware and software. The numbers for higher education are slightly higher than the anticipated increases indicated by 3,000 randomly selected CIOs who participated in the 2003 *CIO Magazine* Tech Poll, which included business and higher education. The poll also revealed that security software is the strongest sector, with 52 percent of the respondents planning to increase spending.

### Sufficiency of Security Funding

We asked respondents whether their institution has provided the needed resources to address IT security issues, using a Likert

scale of 1 to 5. Table 5-11 summarizes the results. The largest percentage thought the institution had not and therefore disagreed (33 percent); a total of 44 percent disagreed or strongly disagreed, 27 percent were neutral, and 28 percent agreed or strongly agreed. The differences among Carnegie classes were small, but college and university system offices and doctoral-intensive institutions expressed the most need.

Finally, we asked for the primary reason the institution uses to justify IT security expenses. Figure 5-15 shows the answers.

In order of frequency are strategic investment (21 percent), incident prevention (17 percent), and reaction to a major incident (16 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 depends, in part, on a reaction to a negative event. We also found that institutions with dedicated security staff were most likely to justify expenditures as major investments. This may explain the higher results for doctoral institutions.

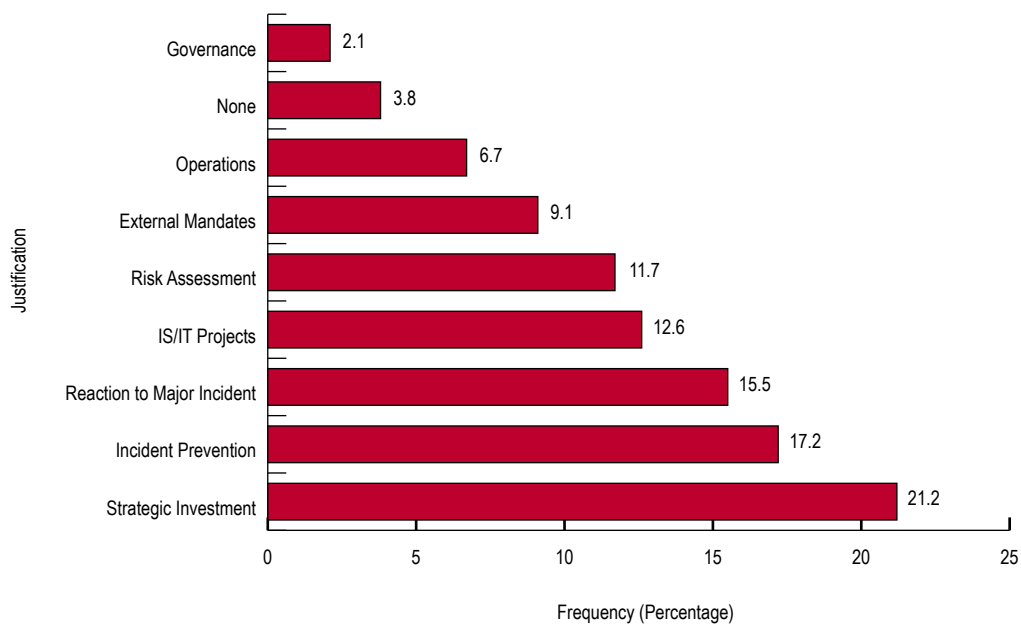
**Table 5-10. Projected Change in IT Security Expenditures**

Change in Expenditure	Target (Percentage of Respondents)			
	Staffing	Hardware/Software	Training	External Services
Significant increase	2.6	9.0	5.4	2.5
Some increase	25.6	38.7	37.0	19.2
About the same	63.3	40.1	43.9	62.3
Some decrease	7.6	10.6	11.1	12.3
Significant decrease	9.0	1.7	2.6	3.7

**Table 5-11. Level of Respondent Agreement on Whether IT Security Funding Is Sufficient, by Carnegie Class and United States Versus Canada**

Carnegie Class and Canada	Mean	Std. Deviation
Dr. Ext.	3.28	0.947
Dr. Int.	3.43	1.065
MA	3.31	1.136
BA	3.10	1.020
AA	3.20	1.030
Specialized	3.25	1.031
System	3.42	1.071
Canada	3.23	1.044

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)



**Figure 5-15. Justification for IT Security Expenditures**

## Endnotes

1. See <<http://infosecuritymag.techtarget.com/2002/aug/securitymarket.shtml>>.
2. D. Ward and B. L. Hawkins, "Presidential Leadership for Information Technology," *EDUCAUSE Review*, Vol. 38, No. 3, May/June 2003, p. 45.
3. For a brief summary of the contents of a security policy, see ISO 17799:2000, p. 2.
4. S. Blake and P. McBride, *Making Security Policies Effective*, BindView Corp., 2002, p. 6.
5. Ibid.
6. Ward and Hawkins, op. cit., p. 45.
7. Ibid., p. 45.
8. See <<http://www.sans.org/resources/mistakes.php>> for common mistakes that organizations can avoid through education.