

Key Findings

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

Judith B. Caruso

Sound information technology security at colleges and universities is essential to protecting information assets, enhancing institutional reputation, and ensuring compliance with state and federal regulations. In recent years, expansion of the Internet has required colleges and universities to increase their attention and investments in IT security to protect institutional infrastructure and intellectual assets. Despite this heightened attention, very little is known about the current state of IT security or about future plans of colleges and universities. This study investigated the state of IT security practices in higher education and compared and contrasted where higher education is relative to industry.

For this study, information security was defined as the preservation of confidentiality, integrity, and availability. Using as a guide the ISO/IEC 17799 framework for security standards from the International Organization for Standardization/International Electrotechnical Commission, the study provides a fact-based perspective of higher education's security environment.

Methodology and Study Participants

This study consisted of five data-collection and analytical initiatives:

- Literature review
- Consultation with a small, select group of IT security leaders in higher education
- A quantitative survey of 435 higher education institutions
- Qualitative telephone interviews with 42 technology executives, managers, and faculty members at 18 institutions
- Four in-depth case studies

The institutions responding to the quantitative study mirror closely the EDUCAUSE membership by Carnegie class. Survey respondents consisted largely of CIOs, chief IT security officers, and other IT staff. Most of the respondents had more than 10 years of experience with IT security.

IT Security Technology Use in Higher Education

Table 1 presents the security approaches identified by survey respondents, in order of use. Secure socket layering (SSL), a centralized data backup, and perimeter firewalls are the most common practices in use or under way, followed by interior firewalls, enterprise directories, virtual private networks (VPNs), and intrusion detection. Shibboleth and electronic signatures are either not under consideration or, at best, 12–24 months out.

Table 1. Status of Security Approaches Used

Security Technology	Adoption Stage (Percentage of Respondents)					
	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
SSL for Web transactions	73.2	12.9	3.1	5.0	3.1	2.6
Centralized data backup	71.0	10.7	2.8	4.2	5.4	5.8
Network firewall (perimeter)	70.9	11.0	2.6	4.4	3.3	7.9
Network firewall (interior)	50.0	18.6	3.8	9.4	8.3	9.9
Enterprise directory	48.2	24.1	4.9	9.1	7.6	6.1
VPN for remote access	45.4	17.8	8.8	12.4	8.1	7.6
Intrusion detection	42.8	15.1	10.4	13.7	15.6	2.4
Intrusion prevention tools	33.1	15.3	10.9	16.1	18.0	6.6
Encryption	31.8	19.5	9.9	9.9	16.6	12.3
Content monitoring/filtering	31.6	10.9	4.9	5.9	10.9	35.8
Standards for application and system development	30.0	21.6	4.1	14.8	12.2	17.3
Electronic signature	6.5	7.8	8.5	10.3	30.5	36.5
Shibboleth	1.1	3.5	4.9	7.1	24.7	58.7

Firewalls are a key technology in higher education. Of all the technologies employed by survey respondents, firewalls were the most commonly used (87 percent). In addition, another 10 percent of respondents are currently installing firewalls. Carnegie class was a significant differentiator regarding perimeter firewall implementation. The most significant difference in technology use among large versus small institutions was in the adoption of SSL for Web transactions. More than 83 percent of doctoral institutions employed SSL, while only 65 percent of other institutions did so.

Higher education appears to employ certain security technologies less often than industry. For example, the 2003 CSI/FBI Computer Crime and Security Survey from the Computer Security Institute—with participation from the San Francisco Federal Bureau of Investigation’s Computer Intrusion Squad—found that 98 percent of industry respondents had installed firewalls versus 87 percent of higher education, as indicated by this survey. In addition, 73 percent of the CSI/FBI respondents use intrusion-detection tools, versus 43 percent in the ECAR survey.

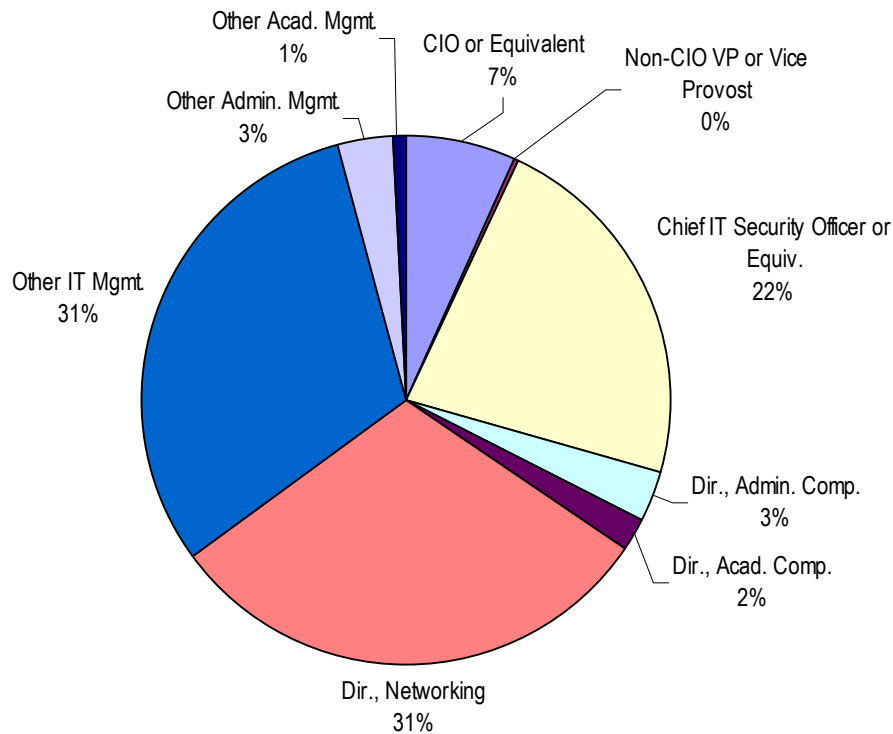
IT Security Management in Higher Education

Security management spans issues of personnel and organization, as well as risk assessment, incident response, and security awareness.

Security Management

According to survey respondents, day-to-day management of IT security is typically the responsibility of central IT organizations, with directors of networking most often in charge, followed by chief IT security officers and CIOs (Figure 1). The position of chief IT security officer has been created largely since 1994, and more than 22 percent of the institutions reporting having the position. The reason for creating the position, however, varies among the institutions.

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



IT Security Staffing

In the recent EDUCAUSE core data survey, institutions reported details about the size of IT security staff. Doctoral institutions employ the most security staff, with an average of 2.5 full-time staff, and baccalaureate institutions average only .37 full-time staff. The number of full-time staff, however, is more closely linked to the number of devices on the network than to Carnegie class. As the number of network devices increases, the number of full-time staff increases, especially as the number of devices rises above 10,000. In the analysis of survey results, the number of dedicated security staff was a significant factor in determining whether security programs are successful. Those institutions employing full-time security staff viewed their security programs as more successful than did those institutions without full-time security staff.

IT Security Policies

Fifty-four percent of the institutions surveyed (235) indicated they had formal institutional policies covering IT security. Of these, 19 percent also had interim policies or policies in progress. Another interesting finding of the study was the importance of the active engagement of institutional senior management in policy development (see Table 2).

Table 2. What Do the Policies Cover? Differences by Carnegie Class

What Formal Policies Cover	Positive Response, by Carnegie Class (Percentage of Respondents)								
	Yes (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
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

IT Security as Institutional Priority

The ECAR survey asked if IT security was one of the top three issues confronting the institutions today. Seventy-five percent of the respondents strongly agreed or agreed. The respondents who strongly agreed were most likely from large doctoral institutions. When asked if IT security was a priority at their institutions, however, only 61 percent strongly agreed or agreed. The gap between security as a top issue and as a priority in higher education is particularly worrisome, given the challenges of ensuring adequate IT security.

IT Security Awareness

Surprisingly, only one-third of the institutions in the study had a formal security awareness program for students and faculty. Doctoral institutions were more likely to have such programs than other institutions. A number of institutions include security-awareness education in student orientation.

Resources

Obtaining adequate financial and human resources for IT security is a challenge for higher education institutions. When asked about the percent of the total IT budget spent on security, 50 percent of the respondents reported that spending on security represented 1–5 percent of the total central IT budget. This amount is significantly less than what is reported by government, banking, telecommunications, and other industries. According to the *Information Week 2002 Global Information Security Survey*, fielded by PricewaterhouseCoopers, businesses spend an average of 12.4 percent of overall IT budgets on security. Differences in how terms are defined across these surveys, however, argue for cautious interpretation of reported variation in investment levels.

IT Security Exposure Practices

All computers connected to a campus network present potential security exposures to the institution. This is an area where most institutions have good practices in place. In the study, 62 percent of the institutions strongly agreed or agreed that they required all campus-owned computers connected to the network to have known security holes fixed. Fifty-nine percent strongly agreed or agreed that their institutions regularly and frequently scan critical systems for known security exposures, but only 40 percent strongly agreed or agreed that their institutions conduct such scans on *all* campus-owned computers connected to the network. Clearly, exposure can be greatly reduced if computers connected to the campus network are scanned regularly for known security exposures.

Incident-Response Procedures

The study asked respondents if they had a formal IT security incident response procedure. Forty-five percent did, with public and doctoral institutions and those with more than 25,000 student enrollments most likely to have these procedures in place. As enrollments increase, so does the likelihood of having a formal incident-response policy. Those institutions with formal incident-response policies in place are able to respond to incidents quickly, ensure that damage assessment is done, and manage internal and external public relations.

Incidents

Only 19 percent of survey respondents reported that they had had an IT security incident that was reported to the press. Larger and doctoral institutions were more likely to have had an incident reported in the press than other institutions. Of the 19 institutions with enrollments of 25,000 or more, 58 percent had an incident reported in the press. As the number of devices and users increases, the percent of institutions that had security incidents reported in the press increases dramatically.

Successful Security Programs

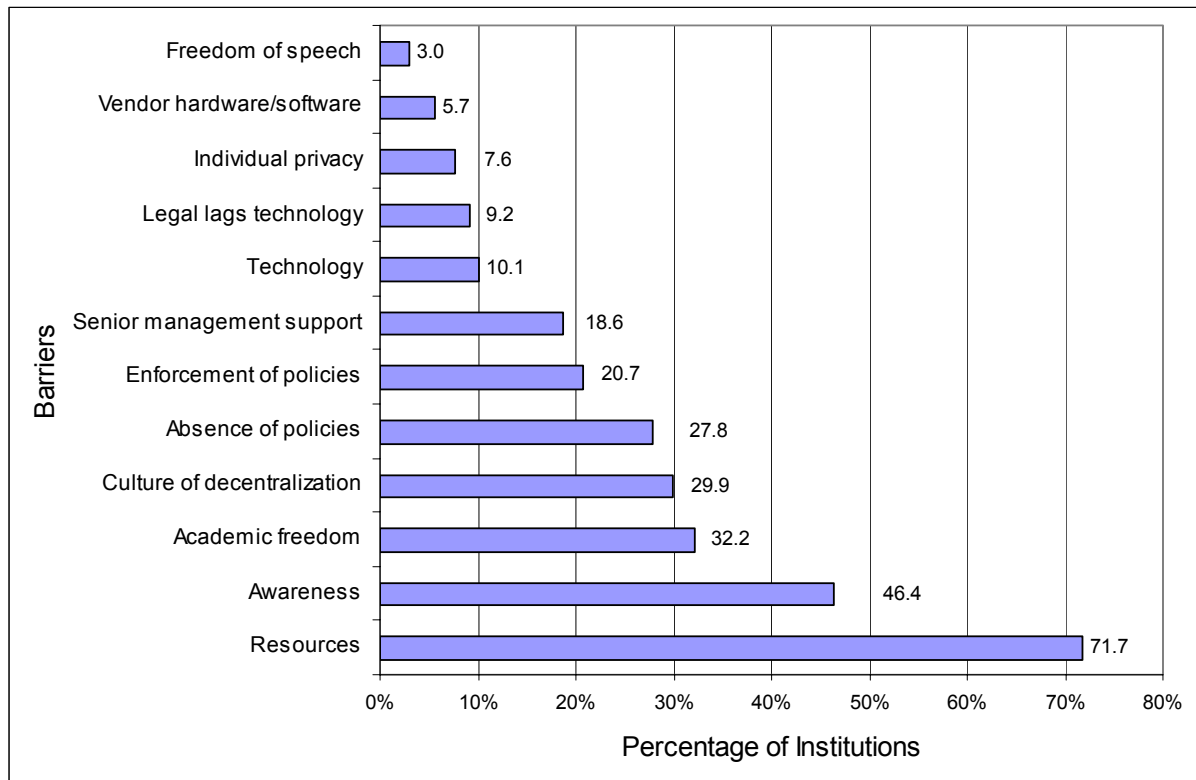
The study asked institutions a number of questions related to measuring the success of their IT security programs. Overall, the respondents felt more secure today than they did two years ago but also felt that their IT security programs need strengthening. Institutions, by and large, have not developed metrics for measuring the effectiveness of their IT security programs. Respondents to the survey who have IT security policies in place, have dedicated IT staff, or include security as a part of their IT plans characterize their IT security programs as successful and feel more secure today than they did two years ago. Also, at institutions where the president and provost are involved in the development of policy, the IT security program is viewed as more successful than at institutions

where they are uninvolved. When IT security policies exist, survey respondents reported feeling that the IT security program was successful.

Barriers to IT Security

The absence of resources was by far the largest barrier to IT security for survey respondents (see Figure 2). Comparing the percent of budget for IT security to the evaluation of success for the IT security program, data show that institutions spending the largest percentage of their total IT budgets on security were the most likely to view their security programs as successful. There is a dichotomy, however, between the perceived importance of IT security and the resources being made available.

Figure 2. Perceived Barriers to IT Security



IT Security—Not Just About Technology

While using technology is necessary to achieve effective security, the human side often needs greater attention. Fifty-two percent of the institutions in the survey strongly agreed or agreed that IT security problems inadvertently caused by authorized users are a significant concern. Despite this, nearly 66 percent of institutions reported having no formal awareness programs in place for students, faculty, and staff. Recommendations from higher education staff emphasize the importance of paying attention to user training and awareness.

Key Questions to Ask

As institutions plan to improve their security efforts, some questions they should ask include:

- What is the institutional culture—centralized or decentralized? How would policy development and security implementation be most effective? Who needs to be involved in policy development and security implementation?
- What is the current state of IT policy and security practice at the institution?
- What technologies are in place? To what level are technologies standardized? Are operating systems and other software at current release levels? Are patches applied regularly?
- How diverse are the users on campus? In addition to basic administrative functions, what are the needs of research and instruction?
- Are residence-hall computers connected to the campus network? What practices and policies address network use?
- What confidential or sensitive data does the institution need to protect? What systems and data are generally open to the public?
- What is the level of security understanding and awareness among students, faculty, and staff? What training and education are needed?
- What are the internal and external threats to the institution? Have any risk assessments been completed? What are the findings of security audits?
- What is the level of understanding and commitment from the president, board of trustees, and provost? What level of engagement is appropriate for the institution?
- What staff and financial resources are available? How can the institution leverage existing funds?
- How can the institution encourage faculty and staff to include security in their IT plans?

Judith B. Caruso (judy.caruso@doit.wisc.edu) is Director of Policy, Security, and Planning at the University of Wisconsin–Madison and Research Fellow at the EDUCAUSE Center for Applied Research.

A copy of the full study referenced above will be available via subscription or purchase through the EDUCAUSE Center for Applied Research (www.educause.edu/ecar/).
