



# Fiscal Year 2004 Summary Report

Brian L. Hawkins, Julia A. Rudy, and Robert Nicolich

September 2005





[www.educause.edu](http://www.educause.edu) • 303-449-4430

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. Membership is open to institutions of higher education, corporations serving the higher education information technology market, and other related associations and organizations. Resources include professional development activities; print and electronic publications, including books, monographs, and the magazines *EDUCAUSE Quarterly* and *EDUCAUSE Review*; strategic policy advocacy; teaching and learning initiatives; applied research; special interest collaborative communities; awards for leadership and exemplary practices; and extensive online information services. The current membership comprises more than 1,900 colleges, universities, and educational organizations, including 200 corporations, with 14,000 active members. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C.; [www.educause.edu](http://www.educause.edu), e-mail [info@educause.edu](mailto:info@educause.edu).

© Copyright 2005 EDUCAUSE

All rights reserved. No part of this monograph may be reproduced in any form without permission in writing from EDUCAUSE.

Art direction by Joseph Daigle, Studio Productions

# FOUR

## Networking, Advanced Technologies, and IT Security

The fourth section of the core data survey focused on networking, methods of remote access, bandwidth shaping, videoconferencing capabilities on campus, deployment of new technologies, and practices related to network security.

### Network Speed and Shaping

The core data survey requested data about the bandwidth available from a campus to the commodity Internet and to high-speed networks. Table 4-1 shows the distinct patterns that characterize bandwidth availability to the Internet by Carnegie groups for responding institutions. Doctoral and OTHER schools have significantly more total bandwidth than MA, BA, and AA colleges, but do not differ significantly from each other. Master's institutions reported significantly more total bandwidth than AA and BA schools. The mean total

bandwidth available to the commodity Internet from campus increased significantly among ALL institutions in the matched data set, up to an average of just over 150 Mbps, an increase of more than 50% since last year. Increases were also found within all groups.

Looking at access to high-performance networks from campuses, Table 4-2 shows that total bandwidth available is related to Carnegie group. The greatest access was reported by doctoral institutions, most likely due to the large data sets, visualization, and other applications needed by faculty at such institutions for their academic work. About 65% of the MA institutions and about three-fourths of the AA and BA colleges responding to our survey provide no access whatsoever to such networks. From 2003 to 2004, the total bandwidth available to high-performance networks increased significantly among ALL institutions in the matched data set

**Table 4-1**  
**Total Bandwidth Available to the Commodity Internet from Campus**

<b>Bandwidth</b>	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
0 Mbps	0.1%	0.0%	0.0%	0.0%	0.6%	0.0%
More than 0–4.5 Mbps	17.3%	0.6%	11.2%	24.3%	34.9%	19.3%
4.6–12 Mbps	20.4%	2.3%	24.1%	32.5%	25.9%	15.7%
12.1–44 Mbps	19.7%	9.2%	27.0%	24.3%	16.9%	17.9%
45–89 Mbps	16.9%	21.8%	20.3%	14.2%	14.5%	10.7%
90–154 Mbps	10.0%	23.6%	5.8%	2.4%	4.8%	15.7%
155–299 Mbps	7.2%	20.1%	6.2%	0.0%	0.6%	9.3%
300–999 Mbps	2.8%	10.9%	0.8%	0.0%	0.6%	2.1%
1,000 Mbps or more	5.6%	11.5%	4.6%	2.4%	1.2%	9.3%

**Table 4-2**  
**Total Bandwidth Available to High-Performance Networks from Campus**

<b>Bandwidth</b>	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
0 Mbps	54.8%	9.2%	64.7%	78.7%	74.1%	42.9%
>0–4.5 Mbps	3.0%	0.0%	4.1%	3.0%	3.6%	4.3%
4.6–12 Mbps	5.6%	4.0%	5.4%	5.3%	8.4%	5.0%
12.1–44 Mbps	4.2%	4.6%	5.4%	0.6%	5.4%	4.3%
45–89 Mbps	9.3%	17.2%	9.1%	7.1%	4.2%	8.6%
90–154 Mbps	3.8%	10.3%	2.5%	1.2%	1.8%	3.6%
155–299 Mbps	6.6%	23.6%	2.5%	1.2%	1.2%	5.7%
300–999 Mbps	2.7%	8.6%	2.1%	0.0%	0.0%	2.9%
1,000 Mbps or more	9.9%	22.4%	4.1%	3.0%	1.2%	22.9%

**Table 4-3**  
**Bandwidth Tracking and Shaping**

<b>Practice</b>	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Track bandwidth utilization	62.8%	62.1%	59.3%	57.4%	68.7%	69.3%
Shape by time of day	25.3%	26.4%	31.5%	34.9%	8.4%	21.4%
Shape by location on campus	48.1%	71.8%	62.7%	57.4%	9.6%	27.9%
Shape by type of traffic	69.9%	77.0%	84.2%	85.8%	37.3%	55.7%
Shape by direction	50.6%	66.1%	60.6%	68.0%	20.5%	28.6%
Do not track or shape	7.9%	2.3%	2.9%	5.3%	18.7%	13.6%

to nearly 294 Mbps, a 70% increase since last year, with doctoral and MA institutions accounting for most of that increase.

Shaping bandwidth refers to adjusting parameters on the campus Internet connection to limit use through various means, such as type of connection, location of connection, direction of traffic, time of day, or other specific characteristics. A campus may choose to shape bandwidth to ensure that the downloading of large files does not interfere with the basic operational needs of the campus and that the bandwidth is available when faculty and students need it for their academic work.

As seen in Table 4-3, about 8% of ALL campuses report not tracking or shaping bandwidth at all, but this percentage is elevated by the high percentage of AA colleges (nearly 19%) reporting no such practices. The dominant strategy of AA colleges appears to be tracking by utilization, with this group reporting much less use of shaping strategies than

the other Carnegie groups. The most popular strategy overall is shaping by the type of network traffic, with AA institutions nonetheless using this strategy far less than doctoral, MA, and BA institutions. Fewer than 9% of AA institutions reported shaping by time of day compared to more than one-third of BA colleges, and only about 20% reported shaping by direction compared to more than 60% for doctoral, MA, and BA schools. Nearly 72% of doctoral institutions reported shaping by location, the highest percentage of all groups.

In looking at the matched data set, there was an increase overall in the past year in the percentage of schools that track bandwidth utilization (from 50.9% to 62.8%). In addition, there was a significant increase in shaping of every kind, for every type of institution, with the notable exception of AA schools, which showed a decrease in shaping by time of day, location, and direction. However, this year fewer AA schools reported no tracking or shap-

**Table 4-4**  
**Level of Remote Access Provided via an Internal Modem Pool to Various Constituencies**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Faculty	49.2%	70.1%	44.0%	52.1%	30.1%	51.4%
Students	35.1%	62.1%	34.9%	33.7%	11.4%	31.4%
Staff	54.3%	74.1%	48.1%	55.0%	40.4%	55.7%
Alumni	6.5%	10.3%	6.6%	7.1%	3.0%	5.0%
Not provided	44.3%	25.9%	49.8%	43.2%	58.4%	42.1%

**Table 4-5**  
**Percentage of Institutions Providing Remote Access to Faculty in Various Ways**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Modem pool	49.2%	70.1%	44.0%	52.1%	30.1%	51.4%
Outsourced modem pool	4.0%	6.9%	2.5%	3.6%	3.6%	4.3%
Institutionally arranged discount with ISP	14.3%	24.7%	12.4%	11.8%	6.6%	16.4%
Subsidized ISP accounts	5.4%	6.3%	4.1%	4.7%	4.2%	8.6%
State academic network	19.6%	25.9%	22.4%	11.8%	16.9%	19.3%
Regional academic network	9.0%	17.8%	5.0%	4.1%	4.2%	16.4%

ing than last year and this group also showed an increase in tracking by bandwidth utilization from last year.

**Remote and Wireless Access**

Providing remote access to the Internet and to campus networks is critical to serving faculty and students who live off campus. The survey asked about six commonly used methods of providing such access to four constituencies: faculty, students, staff, and alumni. Internal modem pool access is differentially employed for various constituencies, as shown in Table 4-4, with the greatest access provided to faculty and staff and considerably less to students. Only 6.5% of ALL respondents make such access available to alumni. The percentage of institutions reporting that remote access is provided via an internal modem pool decreased significantly from 2003 to 2004 for faculty, students, and staff. This is the second year in a row with such decreases, indicating that campuses seem to be moving away from this method.

Table 4-5 shows the percentage of schools providing remote access to faculty in various

ways. Providing access to faculty via an internal modem pool, the strategy employed by about 49% of ALL responding campuses, is the most common method employed. About 4% reported providing access by an outsourced modem pool, and there are no notable differences in the frequency of such offerings across types of institution. Approximately 14% provide access via ISPs with an institutionally arranged discount, while roughly 5% provide subsidized ISP accounts.

The growth of wireless network access on campuses is striking. The 2004 core data survey captured detailed data (far too great to include in this summary report) about the extent of penetration of wireless into eight specified areas of the campus: classrooms, libraries, open spaces, research facilities, administrative buildings, public laboratories, student unions, and residence halls. In general, there is wide variation as to the level of deployment of wireless across these categories and across Carnegie groups. Overall, the highest level of penetration is found in libraries, with more than 57% of ALL respondents

**Table 4-6**  
**Number of Campus Sites from Which Interactive Videoconferencing**  
**Can Be Initiated**

	ALL	DR	MA	BA	AA	OTHER
0	20.0%	1.1%	17.4%	44.4%	18.1%	20.7%
1	15.1%	3.4%	16.6%	27.2%	13.3%	14.7%
2	13.9%	7.5%	17.0%	12.4%	19.9%	11.4%
3	10.4%	6.3%	11.6%	5.9%	14.5%	14.3%
4-5	12.8%	16.7%	14.9%	3.6%	16.3%	11.4%
6-10	14.8%	28.7%	14.9%	4.7%	9.6%	15.7%
11-20	8.1%	22.4%	5.0%	1.2%	5.4%	7.1%
More than 20	4.8%	13.8%	2.5%	0.6%	3.0%	5.0%

**Table 4-7**  
**Percentage of Campus Desktops that Can Deploy Desktop Videoconferencing**

% of Desktops	ALL	DR	MA	BA	AA	OTHER
0%	35.2%	6.9%	36.9%	50.3%	45.2%	37.1%
Up to 19%	45.1%	59.2%	46.5%	34.3%	41.6%	42.1%
20-39%	6.1%	10.9%	4.1%	5.3%	6.6%	3.6%
40-59%	3.9%	8.6%	3.3%	1.8%	2.4%	3.6%
60-79%	3.4%	4.6%	1.7%	4.7%	1.8%	5.0%
80-100%	6.4%	9.8%	7.5%	3.6%	2.4%	8.6%

reporting that 76-100% of their libraries provide wireless access, up 15% from last year. Wireless access is least available in residence halls, open spaces, and research facilities.

### **Videoconferencing Capabilities**

Videoconferencing capabilities were reported by all campus types, but about one-fifth of ALL responding campuses do not have any sites (excluding desktop videoconferencing) from which interactive conferences can be initiated, with that case being most common for BA institutions (about 44%). In addition, the level of penetration varied immensely by Carnegie class, as seen in Table 4-6. More doctoral institutions reported availability of these facilities, with about 14% of respondents in this category having more than 20 such sites.

In addition to central sites for videoconferencing, respondents were asked about the percentage of desktops that could deploy videoconferencing. The same pattern was found as with central sites, with doctoral institutions having the most such capability, followed by

OTHER and MA institutions. As seen in Table 4-7, about half of BA schools reported not having a single machine with such capability.

### **Deployment of New Technologies**

This year's core data survey explored the level of deployment of a dozen technologies that are currently hot topics of conversation within the higher education IT community. This question carried over 10 technologies from last year and added two new technologies (antispam tools and learning objects). Data for these technologies are presented in Tables 4-8 through 4-19.

As shown in Table 4-8, voice over IP (VoIP) technology is being fully deployed at 23.5% of ALL responding campuses. There was a significant increase since last year in the deployment of VoIP for ALL schools and for all groups except doctoral institutions as well as a significant increase in piloting of this technology for ALL institutions.

Video over IP technology is employed to a much higher extent than voice over IP, as

**Table 4-8  
Status of Voice over IP Technology**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	23.5%	27.0%	19.9%	12.4%	29.5%	31.4%
Piloting	16.0%	36.2%	13.7%	10.7%	4.8%	14.3%
In progress	8.8%	9.8%	7.9%	4.7%	12.0%	10.0%
Considering	38.4%	24.1%	44.4%	49.7%	36.7%	34.3%
Not planned	13.4%	2.9%	14.1%	22.5%	16.9%	10.0%

**Table 4-9  
Status of Video over IP Technology**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	39.3%	56.3%	41.1%	16.6%	42.2%	39.3%
Piloting	9.2%	14.4%	6.6%	9.5%	3.0%	14.3%
In progress	11.5%	13.2%	12.9%	7.7%	12.0%	10.7%
Considering	27.8%	14.4%	29.5%	37.9%	30.1%	26.4%
Not planned	12.2%	1.7%	10.0%	28.4%	12.7%	9.3%

**Table 4-10  
Status of PKI Technology**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	15.8%	14.9%	14.1%	12.4%	21.7%	17.1%
Piloting	3.7%	9.2%	2.1%	3.0%	1.2%	3.6%
In progress	6.4%	10.9%	4.1%	5.3%	5.4%	7.1%
Considering	34.0%	46.0%	34.9%	30.8%	22.3%	35.7%
Not planned	40.0%	19.0%	44.8%	48.5%	49.4%	36.4%

shown in Table 4-9. About 39% of ALL campuses reported using this technology, with the highest use by doctoral institutions and lowest use at BA institutions. Associate's colleges are second highest in reporting use of this advanced technology, probably in large part due to their innovative use of technology in teaching and learning. The use of this technology increased since last year, and there was a decrease in those not planning to implement video over IP.

The use of public key infrastructure (PKI) is interesting to note, as this technology may well be critical in the deployment of campus security policies and practices. As seen in Table 4-10, deployment of PKI is still in the early stages of diffusion, despite the amount of campus discussion and numbers of conference presentations on this topic. There was virtually no

change in the level of deployment, piloting, or progress in deployment of PKI since last year, the second straight year of no movement on use of this technology.

Doctoral institutions use enterprise directory technology more than the other types of institution, but as of this year, more than half of responding institutions in all groups are using it. Such a directory is essential for the authentication and authorization efforts required in PKI. As shown in Table 4-11, the vast majority of respondents have already deployed it, are considering it, or are in the process of implementing it. Overall, there was a significant increase in the deployment of enterprise directory technology since last year.

There is still very little deployment of biometric technology on campuses, which includes use of fingerprints, retinal scans, or

**Table 4-11**  
**Status of Enterprise Directory Technology**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	63.1%	77.0%	61.8%	56.2%	51.2%	70.7%
Piloting	3.4%	3.4%	3.7%	4.1%	1.8%	3.6%
In progress	14.9%	15.5%	21.2%	13.6%	9.6%	11.4%
Considering	9.9%	2.9%	9.1%	9.5%	18.1%	10.7%
Not planned	8.7%	1.1%	4.1%	16.6%	19.3%	3.6%

**Table 4-12**  
**Status of Biometric Technology**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	2.7%	5.7%	2.5%	1.8%	1.2%	2.1%
Piloting	3.3%	5.7%	4.1%	0.6%	0.6%	5.0%
In progress	1.6%	3.4%	0.8%	0.6%	1.2%	2.1%
Considering	21.7%	30.5%	19.9%	17.2%	19.3%	22.1%
Not planned	70.8%	54.6%	72.6%	79.9%	77.7%	68.6%

**Table 4-13**  
**Status of Smart Card Technology**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	18.7%	25.3%	20.3%	21.3%	4.8%	20.7%
Piloting	2.5%	4.0%	1.7%	2.4%	1.2%	3.6%
In progress	6.2%	6.3%	6.6%	5.3%	5.4%	7.1%
Considering	35.6%	36.8%	33.6%	36.1%	34.3%	38.6%
Not planned	37.1%	27.6%	37.8%	34.9%	54.2%	30.0%

other physiological means of user identification for security purposes. Over 70% of ALL responding campuses are not even planning for this technology (see Table 4-12), but there were significant increases in the number of ALL campuses piloting and considering biometrics since last year.

As shown in Table 4-13, the deployment of smart cards was reported most by doctoral institutions and least by AA institutions. Only about 19% of ALL responding institutions reported deployment of smart card technology, and more than 37% reported that this technology is not planned. There was a significant increase in deployment of this technology since last year for ALL respondents, with most of the change occurring in BA institutions.

Web services technology refers to a set of tools and building blocks for system develop-

ment. As shown in Table 4-14, this technology is relatively advanced at a large percentage of institutions overall and within each Carnegie class. Nearly 74% of doctoral institutions have deployed Web services technology, and another 13.8% are piloting it or have it in progress. Among BA and AA colleges, 57.4% and 55.4%, respectively, have deployed this technology, and about another 15% of these institutions are piloting this technology or have it in progress. Overall, the deployment of this technology increased significantly from 2003 to 2004 for ALL institutions, and the percentage of ALL respondents reporting no plans to deploy this technology decreased significantly.

While the status of the various technologies discussed thus far has differed considerably across Carnegie groups, antivirus software was reported to be deployed at nearly 99% of ALL

**Table 4-14**  
**Status of Web Services Technology**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	63.3%	73.6%	67.6%	57.4%	55.4%	59.3%
Piloting	3.8%	6.3%	3.3%	3.0%	3.0%	3.6%
In progress	10.2%	7.5%	6.6%	11.8%	11.4%	16.4%
Considering	14.6%	10.9%	11.6%	18.9%	16.9%	16.4%
Not planned	8.1%	1.7%	10.8%	8.9%	13.3%	4.3%

**Table 4-15**  
**Status of Antivirus Software**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	98.9%	98.3%	98.3%	99.4%	99.4%	99.3%
Piloting	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
In progress	1.0%	1.7%	1.2%	0.6%	0.6%	0.7%
Considering	0.1%	0.0%	0.4%	0.0%	0.0%	0.0%
Not planned	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

**Table 4-16**  
**Status of Electronic Signatures**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	7.4%	6.3%	7.9%	7.1%	7.2%	8.6%
Piloting	4.6%	9.2%	5.4%	1.8%	3.0%	2.9%
In progress	7.2%	9.8%	7.9%	4.7%	3.6%	10.0%
Considering	44.6%	55.7%	44.8%	36.1%	43.4%	42.1%
Not planned	36.2%	19.0%	34.0%	50.3%	42.8%	36.4%

**Table 4-17**  
**Status of Wireless Security Technologies**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	49.8%	69.0%	51.0%	41.4%	36.1%	50.0%
Piloting	11.2%	12.1%	12.4%	10.1%	10.2%	10.7%
In progress	19.2%	14.4%	15.4%	21.3%	25.9%	21.4%
Considering	17.2%	4.0%	17.4%	25.4%	24.7%	14.3%
Not planned	2.6%	0.6%	3.7%	1.8%	3.0%	3.6%

responding institutions and by at least 98% of institutions within each group. Table 4-15 shows the remarkable consistency and high level of deployment of antivirus software.

Like biometrics, electronic signature technology is not particularly common in higher education institutions across all groups, as shown in Table 4-16. Again, the percentage of campuses at which such technology has been

deployed, is in the pilot stage, or is otherwise in progress is greatest for doctoral institutions, at about 25%, followed by approximately 21% of MA and OTHER colleges. This technology is not even planned at more than 36% of ALL institutions.

Table 4-17 shows the status of wireless security technologies to be particularly advanced at doctoral institutions, with 69%

**Table 4-18**  
**Status of Antispam Tools**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	79.6%	88.5%	79.7%	76.9%	71.1%	81.4%
Piloting	4.4%	2.3%	3.7%	5.9%	4.2%	6.4%
In progress	8.7%	5.2%	11.2%	9.5%	10.2%	5.7%
Considering	6.5%	3.4%	5.0%	7.1%	12.7%	5.0%
Not planned	0.9%	0.6%	0.4%	0.6%	1.8%	1.4%

**Table 4-19**  
**Status of Learning Objects**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Deployed	9.8%	12.1%	7.9%	5.3%	13.9%	10.7%
Piloting	4.7%	6.9%	5.8%	3.6%	3.0%	3.6%
In progress	11.9%	14.4%	8.7%	10.1%	12.0%	16.4%
Considering	34.0%	33.9%	35.3%	31.4%	30.1%	40.0%
Not planned	39.6%	32.8%	42.3%	49.7%	41.0%	27.3%

reporting having deployed this technology and less than 1% reporting no plans for implementing it. Another 26.5% of doctoral schools are piloting this technology or have it in progress. About half of MA and OTHER colleges have deployed wireless security technologies, as have about 36% of AA institutions, the lowest percentage among the Carnegie classes. There was a significant leap in deployment of this technology since last year, with an approximately 15% increase in deployment overall and significant increases in every type of institution.

This year's survey captured data about an additional new technology, antispam tools. As seen in Table 4-18, nearly 80% of ALL respondents reported having deployed this technology, with doctoral institutions having deployed it most (88.5%) and AA schools least (about 71%). The other new technology included on this year's survey was learning objects, which appears to be rarely deployed at this time, as illustrated in Table 4-19. Nearly 40% of ALL respondents and nearly 50% of BA colleges have no plans for using this technology. However, 34% of ALL respondents are considering implementing learning objects, so this technology will bear watching in the future.

### **Security**

The final area of analysis in this section is security, including the processes being used to secure campuses from disruptions of service, incursions, and other security breaches. Perhaps the most common type of security protection being used by responding campuses is a firewall. However, experience has shown that a single firewall is not adequate for security because many of the individuals who provide a threat to security are students and personnel who work and operate within the environment protected by the firewall. Table 4-20 shows various strategies currently being employed and their relative frequency within each of the Carnegie groups.

Overall, less than 1% of ALL respondents have no firewalls, with the most common strategy being the deployment of a firewall at the external Internet connection. Overall, the percentage for the latter is up significantly, from 82% last year to 86.6% this year. This is true for a very large percentage of schools in all categories except doctoral institutions, which more often reported deploying firewalls around high-security servers and by or for individual departments.

Table 4-21 shows the patterns and use of software patches and other practices to ensure

**Table 4-20  
Campus Firewall Strategies**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Firewall at external Internet connection	86.6%	64.4%	92.5%	91.1%	94.0%	90.0%
Firewalls around certain high-security servers or networks	61.1%	87.4%	67.2%	46.2%	39.8%	61.4%
Firewalls deployed by or on behalf of individual departments	33.6%	77.0%	31.5%	11.2%	13.9%	33.6%
Campus site license for a personal firewall product	14.0%	19.5%	17.0%	7.7%	10.2%	14.3%
Plan to implement one or more firewalls	17.6%	30.5%	17.4%	9.5%	10.8%	20.0%
No firewalls	0.7%	0.7%	0.0%	0.6%	1.2%	0.6%

**Table 4-21  
Security-Related Practices**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
All critical systems expeditiously patched or updated	96.5%	95.4%	97.5%	98.2%	95.8%	95.0%
Campus computers expeditiously patched or updated	82.2%	73.0%	88.0%	87.0%	80.1%	80.7%
Personal computers expeditiously patched or updated	46.2%	50.6%	53.5%	54.4%	21.7%	47.1%
Proactive scans in critical systems	74.3%	87.9%	78.0%	71.0%	60.8%	70.7%
Proactive scans in campus computers connected to the network	63.1%	72.4%	66.4%	56.2%	56.6%	62.1%
Proactive scans in PCs connected to the network	38.7%	54.0%	42.3%	40.8%	17.5%	35.7%
Security system includes intrusion detection system	49.6%	72.4%	50.2%	35.3%	35.5%	53.6%

security on campus. Far and away the most common practice is requiring all critical systems to be expeditiously patched or updated, with this being reported by 96% of ALL respon-

dents and no significant differences among Carnegie groups for this practice.

The second most common practice is requiring campus-owned or -leased computers to be

**Table 4-22  
Security Policy Advisory Participants**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
IT policy/security officer	64.0%	82.8%	57.3%	49.1%	59.6%	75.7%
CIO/central IT organization representative	95.5%	99.4%	97.9%	92.3%	90.4%	96.4%
Auditor	43.7%	72.4%	42.7%	21.3%	30.1%	52.9%
General counsel	53.3%	89.1%	56.0%	35.5%	30.7%	52.1%
Chief financial officer	57.3%	63.2%	63.5%	52.7%	50.0%	53.6%
Chief academic officer	54.8%	65.5%	56.8%	50.9%	51.2%	47.1%
Campus police	17.1%	27.0%	20.3%	11.8%	13.3%	10.0%
President's cabinet	63.1%	59.2%	68.5%	60.4%	72.3%	51.4%
Board of trustees	13.7%	20.7%	13.3%	10.1%	12.7%	11.4%
Campus task force	25.5%	50.0%	19.5%	14.2%	22.3%	22.9%
Technology advisory committee	64.6%	67.2%	63.1%	62.1%	66.9%	64.3%
Faculty committee	33.1%	47.7%	37.3%	27.8%	22.3%	27.1%
State agency/system office	21.6%	25.9%	25.3%	6.5%	33.7%	13.6%
No policy development	0.7%	0.0%	0.4%	0.0%	1.8%	1.4%

expeditiously patched or updated, with about 82% of ALL respondents reporting this practice. Conducting proactive scans to detect known security exposures in critical systems is the third most common practice, with nearly three-fourths of ALL respondents reporting this. The least reported practice is conducting proactive scans to detect known security exposures in all personally owned computers connected to the campus network, reported by about 39% of ALL respondents.

Overall, there is an overwhelming increase in security-related practices when compared to last year, and this increase is nearly universal across all Carnegie groups. The only practice that did not show a significant net increase is requiring all critical systems to be expeditiously patched or updated, but this practice was already overwhelmingly in place, at 95.5% last year compared to this year's 96.5%.

In an earlier section of the survey, respondents were asked to identify the participants in policy development related to security on campus. These data are reported here for their synergy to security-related practices. As shown in Table 4-22, the patterns of involvement and

the breadth of participation in such policy efforts varied dramatically across Carnegie groups, except for one area. In all cases, the CIO or central IT organization representative is the most common participant in such processes, with about 96% of ALL respondents checking this option and more than 90% of the schools in each group reporting this engagement. A significantly higher percentage of doctoral institutions than other types of school reported involvement of the IT policy/security officer, the general counsel, the auditor, and a campus task force. The president's cabinet was reported to be used considerably more than other groups by AA colleges. Fewer BA institutions than schools in any of the other groups reported engaging an IT policy/security officer, auditor, campus task force, or state agency.

Finally, this year's survey asked a new question to collect data about how many campuses have actually undertaken an IT security risk assessment. As seen in Table 4-23, 52% of ALL campuses responded in the affirmative. Looking at the Carnegie groups, some significant differences are apparent. Doctoral insti-

**Table 4-23**  
**Campus IT Security Risk Assessment**

	<b>ALL</b>	<b>DR</b>	<b>MA</b>	<b>BA</b>	<b>AA</b>	<b>OTHER</b>
Yes	52%	70.1%	53.5%	36.7%	40.4%	59.3%
No	48%	29.9%	46.5%	63.3%	59.6%	40.7%

tutions have undertaken risk assessments at a much higher rate than other groups (more than 70%), with BA and AA colleges the only

groups in which more than half of the respondents reported not having conducted such an assessment.