

4

IT Security Technologies Implemented by Higher Education Institutions

If a great many remedies are suggested for a disease, it means the disease is incurable.

—Anton Chekhov

This chapter explores the information security technologies used by the institutions in our survey. What tools have they chosen to install to prevent harm to their information assets? Do we find differences among the institutions? For example, do institutions with many devices on their networks pursue different IT security strategies than those with fewer devices? Are there differences among Carnegie class institutions? And how does higher education compare with industry? Is it true that higher education lags the private and corporate sectors in installing security technologies?

We define the technologies discussed here by functionality, locus or scope of use, objectives, and the threats they address.¹

Security Technologies in Use

The data we collected portray a fairly comprehensive view of security approaches that our subset of higher education institutions currently have in place, are implementing, or are piloting to prevent cyber attacks. We asked institutions in the planning stage when they expect to undertake various se-

curity approaches. We also determined if an approach was even under consideration.

Table 4-1 presents the data in rank order of use. Secure Sockets Layer (SSL), centralized data backup, and perimeter firewalls are most in use or under way, followed by interior firewalls, enterprise directories, virtual private networks (VPNs), and intrusion detection. For most institutions, electronic signatures are either not under consideration or at best are 12 to 24 months out. While the data for Shibboleth² are similar, its adoption rate is increasing since we completed the survey.

Not surprisingly, we find a great emphasis on firewalls combined with antivirus software as a solution to network security. This combination is used by 97 percent of the ECAR survey institutions. Fully 87 percent of the institutions responding to the survey have installed either an interior or perimeter firewall or both. Another 10 percent are currently installing firewalls, which will bring these higher education institutions to the level other survey data show for industry. Of the institutions that have implemented interior firewalls, 80 percent have also installed

Table 4-1. 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

perimeter firewalls. Of the institutions that have installed perimeter firewalls, 56 percent have also installed interior firewalls. The 2002 EDUCAUSE Core Data Service survey corroborates these findings.

Firewalls, however, have their problems and trade-offs. According to Terry Gray, University of Washington, "firewalling," or perimeter protection, "is about *policy-based*

packet filtering at specific physical or logical points in a network—that is, blocking certain packets from proceeding to their intended destination. It is a defensive strategy implemented at the network transport layer of a system hierarchy. Sometimes the implementation is done on the host and sometimes it is part of the network infrastructure itself." Gray further noted that "a growing num-

ber of security professionals recognize that a network-centric approach to security is at best inadequate and at worst dangerous if it lessens focus on host security—especially in an environment where vast numbers of quasi-independent units with wildly differing computing needs share the same network infrastructure.”

On a further note of caution, Gary Dobbins, director of information security, University of Notre Dame, stated, “Selecting the technology or overall strategy is not the difficult aspect of the job. Integrating it with current or future practices is the lion’s

share of the work there. For example, fitting a firewall into an existing data center without disrupting current services, and retraining and realigning processes and procedures around it can take a great deal of time and effort as well.”

Interior Versus Perimeter Firewalls

Baccalaureate institutions (83 percent) were twice as likely as doctoral institutions (40 percent) to have perimeter firewalls (see Table 4-2).

Table 4-2. Security Approaches Adopted, by Carnegie Class and Canada

Security Approach	Adoption, by Carnegie Class (Percentage of Respondents)							
	Dr. Ext.	Dr. Int.	MA	BA	AA	Special	System	Canada
SSL for Web transactions	81.8	85.7	68.2	67.1	60.0	66.1	73.7	85.7
Centralized data backup	61.8	77.1	69.1	72.1	78.0	66.1	84.2	61.9
Network firewall (perimeter)	40.3	62.9	76.6	82.6	76.5	82.1	52.6	76.2
Network firewall (interior)	49.4	51.4	48.6	51.8	35.3	12.5	15.8	66.7
Enterprise directory	48.1	48.6	38.0	52.3	44.0	58.2	11.1	52.4
VPN for remote access	53.2	48.6	38.2	38.4	34.0	56.4	52.6	57.1
Intrusion detection	53.2	54.3	31.8	38.8	33.3	53.6	31.6	42.9
Intrusion prevention tools	34.2	42.9	24.8	35.7	25.5	38.2	21.1	25.0
Encryption	32.5	37.1	25.7	37.6	33.3	35.7	15.8	23.8
Content monitoring/filtering	19.5	40.0	26.6	36.5	33.3	35.7	15.8	23.8
Standards for application and system development	19.5	31.4	29.4	31.8	18.0	34.5	26.3	25.0
Electronic signature	9.1	8.6	3.7	4.7	6.0	7.1	5.3	4.8
Shibboleth	2.6	0.0	0.0	1.2	0.0	0.0	0.0	0.0

Perimeter firewalls were more often found at smaller enrollment institutions (see Table 4-3). For example, 80 percent of institutions with 4,000 or fewer students had perimeter firewalls versus 50 percent of institutions with 15,001 or more enrolled students. By contrast, interior firewalls were more often in place at larger institutions, where 74 percent of institutions with more than 25,000 enrolled students have interior firewalls versus approximately 48 percent for everyone else.

Sixty-eight percent of Canadian institutions had interior firewalls versus 48 percent of U.S. institutions. In general, a higher percentage of Canadian institutions employed

security approaches—and most employed more—than their U.S. counterparts. Canadian institutions, as a group, look more like the U.S. doctoral-extensive Carnegie class than they do smaller U.S. institutions.

Terry Gray described the large-school strategy: “Border firewalls have some long-term negative consequences, such as encouraging people to tunnel all manner of applications through ports that are rarely blocked by firewalls, and increasing the time it takes to troubleshoot problems with networked applications.”³ He suggested a strategy of “open networks, closed servers, and protected sessions,” by which he means pushing security perimeters and policy defini-

Table 4-3. Security Approaches Implemented, by Institution Size (Student Enrollment)

Security Approach	Adoption, by Institution Size (Percentage of Respondents)					
	Up to 2,000	2,001 to 4,000	4,001 to 8,000	8,001 to 15,000	15,001 to 25,000	25,001 or More
SSL for Web transactions	57.3	65.9	77.2	75.8	86.3	89.5
Centralized data backup	66.9	71.8	70.9	72.6	70.0	63.2
Network firewall (perimeter)	79.6	86.2	72.2	53.2	49.0	52.6
Network firewall (interior)	44.9	50.0	46.8	53.2	43.1	73.7
Enterprise directory	44.0	45.9	46.2	53.2	49.0	52.6
VPN for remote access	38.1	44.0	41.8	43.2	47.1	63.2
Intrusion detection	34.7	43.5	36.7	46.8	51.0	68.4
Intrusion prevention tools	32.5	32.9	26.0	30.6	36.0	47.4
Encryption	29.9	32.1	30.4	27.4	31.4	47.4
Content monitoring/filtering	31.6	37.3	25.3	37.7	17.6	26.3
Standards for application and system development	27.1	28.6	26.9	29.0	28.0	21.1
Electronic signature	6.8	3.5	6.3	6.5	3.9	15.8
Shibboleth	0.9	0.0	0.0	0.0	2.0	5.3

tion as close as possible to the organizations and computers to be protected, and making sure all sensitive traffic is encrypted. A one-size-fits-all strategy is problematic for the research university, and this approach serves the reality of the large institution. Tighter security is achieved by tailoring security to specific applications or needs of each small group or individual. Jeffrey Schiller, network manager at the Massachusetts Institute of Technology, agreed with this approach, saying, "Firewalls work best the closer they are to the assets they protect."

Perimeter firewalls make sense at institutions where there are "homogeneous and simple computing requirements, the enterprise firewall is viewed solely as a defense-in-depth strategy, desktop configurations are tightly controlled by a central entity, and where performance and reliability concerns have been adequately addressed," said Gray. He added that the research university fails this suitability test on all counts. However, the smaller institution, which quite often will not have the same level of IT resources as a large research institution, nor the same complex demands on its network, may well be served by a professionally managed perimeter firewall, which can reduce the amount of work needed to secure the rest of the institution's network. Schiller warned, however, that "Firewalls can engender a false sense of security. A purchased firewall is not a substitute for professional [IT security] staff."

Other Data Protection Strategies

The largest institutions were more likely to use enterprise directories, encryption, VPN, and electronic signatures, although we did find that 37 percent of institutions in every Carnegie class were not considering electronic signatures.

A VPN uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. It differs from an expensive system of owned or leased lines that only one organization can use. It works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, by encrypting data at the sending end and decrypting it at the receiving end, the protocols send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses.

VPNs were in place at 63 percent of institutions with more than 25,000 enrolled students, compared with 40 percent for every other enrollment grouping. Fifty-seven percent of the Canadian institutions had installed VPNs versus 45 percent in the United States.

Shibboleth is developing architectures, policy structures, practical technologies, and an open-source implementation to support interinstitutional Web resource sharing subject to access controls. Using Shibboleth, the origin campus (home to the browser user) provides attribute assertions about that user to the target site. A trust fabric exists between campuses, allowing each site to identify another's users and assign a trust level. Origin sites are responsible for authenticating their users but can use any reliable means to do this. Access-control decisions are made using the assertions. The origin site and the browser user control what information is released to the target.

Use of a centralized data backup system was lowest in doctoral-extensive institutions (62 percent versus 71 percent in general),

which is not surprising given the decentralized nature of computing at many institutions in this class. And this was one area where Canadian institutions lagged their U.S. counterparts (62 percent versus 71 percent).

Perhaps the most significant difference between large versus small institutions and doctoral versus other Carnegie class institutions concerned the use of SSL. This protocol uses encryption to secure communications between Web browsers and servers. Eighty-eight percent of institutions with more than 15,000 students had SSL; this dropped to a

low of 57 percent at institutions with enrollments of 2,000 and under. Eighty-three percent of doctoral institutions had SSL versus 65 percent for everyone else, and 85 percent of Canadian institutions had SSL versus 73 percent in the United States. Intrusion detection and intrusion prevention tools follow a similar pattern. We are unsure whether this difference is due to expense or perceived complexity, or because smaller institutions are less likely to have Web-enabled applications that require secure connectivity.

Table 4-4 shows the rank order of strategies used by institutions in each Carnegie

Table 4-4. Security Approach Rankings, by Carnegie Class and Canada

Security Approach	Rank, by Carnegie Class					
	Dr. Ext.	Dr. Int.	MA	BA	AA	Canada
SSL for Web transactions	1	1	3	3	3	1
Centralized data backup	2	2	2	2	1	4
Network firewall (perimeter)	3	3	1	1	2	2
Network firewall (interior)	4	5	4	5	5	3
Enterprise directory	5	6	6	4	4	6
VPN for remote access	6	7	5	7	6	5
Intrusion detection	7	4	7	6	7	7
Intrusion prevention tools	8	8	11	10	10	8
Encryption	9	10	10	8	8	9
Content monitoring/filtering	10	9	9	9	9	10
Standards for application and system development	11	11	8	11	11	11
Electronic signature	12	12	12	12	12	12
Shibboleth	13	13	13	13	13	13

class and in Canada. It confirms perhaps more clearly the different approaches each subgroup is taking. The differences are small, with the major difference being the use of SSL and firewalls.

In summary, we found larger institutions (in terms of student enrollment) and Carnegie doctoral-extensive institutions more likely to have employed more of the available technology strategies, with a major difference in the use of perimeter firewalls. Institution size probably predicts what has been installed better than Carnegie class. A similar pattern occurs when we look at the number of users and devices on the network. For example, perimeter firewalls are used by 80 percent of institutions with 5,000 or fewer devices. But no institution in our survey with more than 100,000 devices used perimeter firewalls, and only 20 percent of the institutions with 80,001–100,000 devices employed them. Note, however, the small number of such institutions in our study. The number of devices differentiates

institutions more strongly than number of users on the network.

Higher education rates somewhat lower in the use of these technologies than industry, as shown in Table 4-5. The table arrays survey findings from the ECAR survey; the 2003 CSI/FBI Computer Crime and Security Survey, sponsored by the Computer Security Institute; the 2003 Healthcare Information and Management Systems Society (HIMSS) Leadership Survey; and a 2002 KPMG survey. Note that these surveys' methodologies, definitions, and sample sizes varied greatly, and the comparisons should be read with caution. Also, these surveys are snapshots in time of an environment that is rapidly and dynamically changing and where today's preferred IT security technologies may quickly become obsolete. Adoption patterns may reflect this reality, especially where resources are limited.

The CSI/FBI survey found that 98 percent of their respondents had installed firewalls versus 87 percent in our study, and 73 per-

Table 4-5. Comparing Higher Education Security Approaches with Industry Study Results

Security Approach	Survey Population (Percentage of Respondents)			
	ECAR	CSI/FBI	HIMSS	KPMG
Antivirus software	97	99		
Network firewall	87	98	98	
Intrusion detection	43	73		15
Encryption	32	69	65	
Electronic signature	7		56	

cent used intrusion detection tools versus 43 percent in our study.⁴ The HIMSS survey indicated that 98 percent of the medical institutions used firewalls. More remarkable is that 56 percent used electronic signatures versus 7 percent for higher education, and 65 percent used data encryption versus 32 percent in our survey. However, a 2002 KPMG survey showed that only 14 percent of the respondents run a network-based intrusion detection system, and 15 percent run a host-based intrusion detection system.⁵

Writer Jon Surmacz reports on security detection in the private sector. Using findings from a 2002 Top Layer Networks survey of 809 business professionals, mostly from private industry,⁶ he noted that 42 percent of respondents have intrusion detection systems, which is similar to the usage reported by our institutions.

What these data show is that the ECAR survey institutions are fairly comparable to industry in the use of firewalls and antivirus software. But our data also show that many ECAR survey institutions are in the process of implementing these technologies. This lag may be due to cost, but it may also be due to risk and the kind of data that need to be protected. The CSI/FBI survey noted that the greatest financial losses to businesses surveyed were from the theft of proprietary information (\$70 million), denial of service (\$65 million), and viruses (\$27 million). Quite frankly, the first two risk areas do not have the same impact on higher education. Much of higher education's information is public, and denial-of-service attacks, while inconvenient, would not devastate universities financially as they would an eBay or Amazon. It would cause dissatisfaction if registration, for example, were delayed a day or two, but teaching, research, and

other core institutional functions could for the most part continue uninterrupted. Thus it may not make sense for higher education to invest as heavily as industry in some of these IT security technologies. The return on investment and perceived risk level may be too low to justify the investment. If this is true, the argument that higher education is under invested in security technologies may simply not be justified. The answer may be that higher education institutions face a different risk profile and therefore require a somewhat different set of solutions.

Remote Network Access

Eighty-two percent of the institutions reported providing remote network access (see Figure 4-1). Public institutions (85 percent) are slightly more likely to provide remote access than private institutions (77 percent). Eighty-six percent of Canadian institutions provide remote access. All but two of the doctoral institutions provide remote access; two-thirds of the associate's institutions provide remote access.

Seventy-six percent of the institutions (267 of 350 institutions responding to this part of the survey) provide a campus modem pool; 8 percent outsource; 26 percent arrange for a discount with an ISP; and 18 percent provide subsidized ISP accounts (Figure 4-2). We found only minor differences between public and private institutions.

Some institutions provide different services to faculty, staff, and students—for example, the campus modem pool may not be open to students, who would then purchase Internet service from a private ISP. In some instances, the campus pool is so limited that users go outside. And users will also go outside to get greater bandwidth. The University

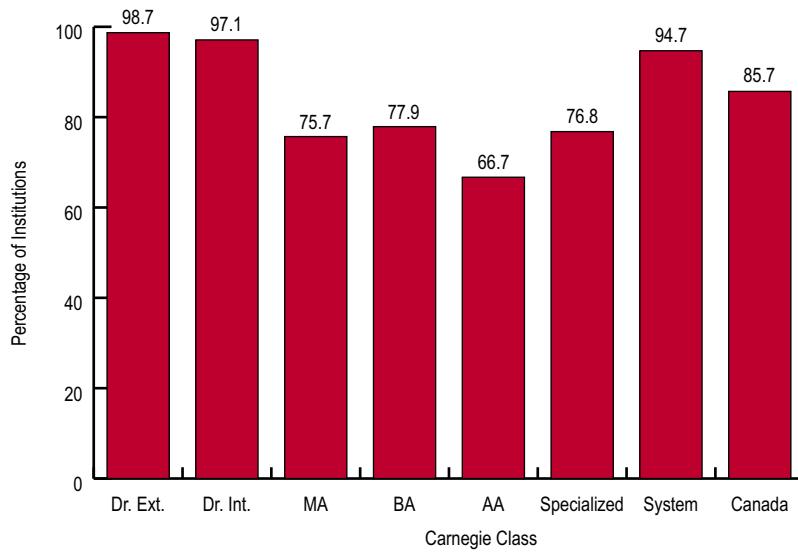


Figure 4-1.
Provision of Remote Access, by Carnegie Class

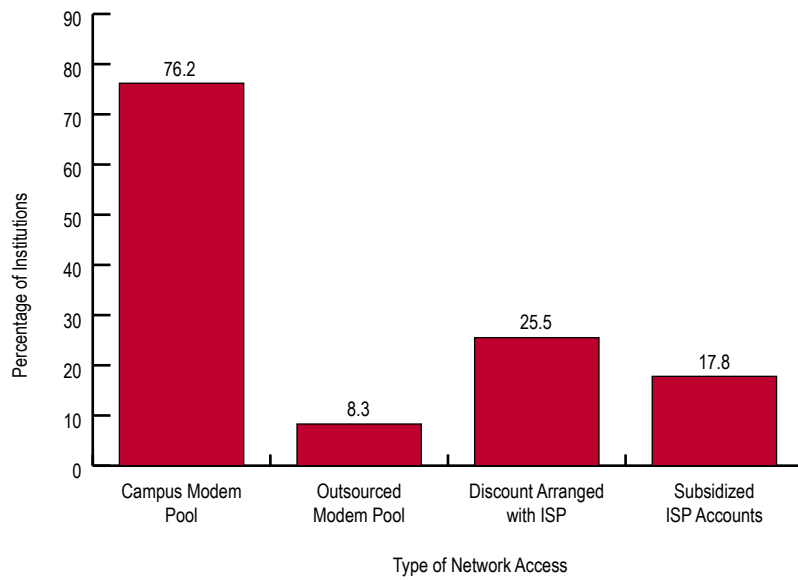


Figure 4-2.
Network Access Provided by Institutions

of Minnesota, Twin Cities, for example, has negotiated a discount with an outside provider for students, faculty, and staff to obtain DSL or cable services at home.

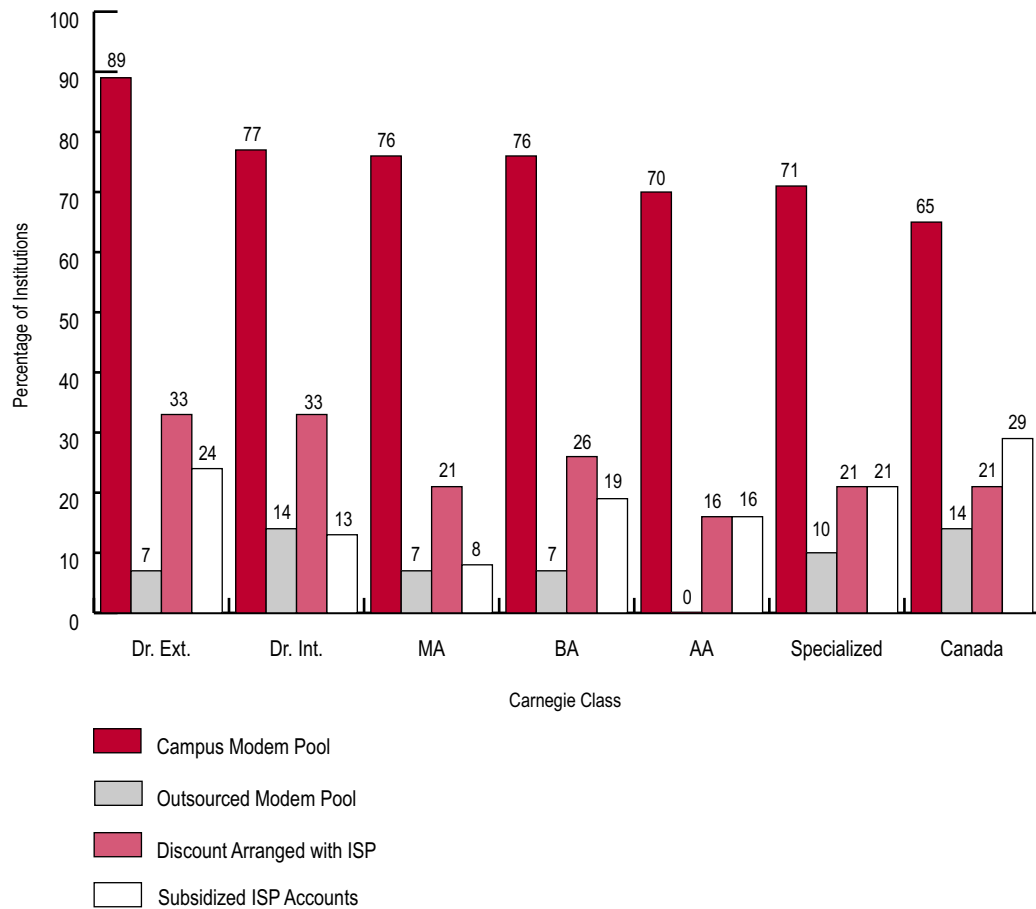
We found some variation among the different Carnegie classes (see Figure 4-3). Doctoral-extensive institutions were most likely to have a campus modem pool (89 percent), and Canadian institutions were least likely (65 percent). Canadian and doctoral-intensive institutions were most likely to outsource, but the numbers are low. In

addition, Canadian institutions were most likely to subsidize ISP accounts.

Wireless Security

Eighty-eight percent of institutions surveyed reported that wireless technology was installed on campus. The larger the institution's enrollment, the more likely it had installed wireless technology. Seventy-eight percent of institutions with enrollments of less than 2,000 students reported that they provide wireless access, whereas 100

Figure 4-3.
Network
Access, by
Carnegie Class



percent of the institutions with enrollments over 15,000 did so. Carnegie class shows a similar pattern. All doctoral institutions, save one, report having wireless, compared with 78 percent of associate's institutions. We noted a significant difference here with industry: the KPMG survey reported that only 10 percent of their participating firms have installed wireless networks.

Table 4-6 shows the status of technologies to secure wireless installations. Large institutions differ from smaller institutions, and doctoral institutions differ from master's, baccalaureate, associate's, and, to some degree, Canadian institutions in the use of strategies to secure wireless network access. Extensible authentication

protocol (EAP), 128-bit wired equivalency privacy (WEP), and firewalls are more often used at master's, baccalaureate, associate's, and, to some extent, Canadian institutions. IP VPNs, Kerberos, and remote authentication dial-in user service (RADIUS) prevail at large-enrollment and doctoral institutions. Otherwise the usage pattern is similar for all institutions, with the seeming anomaly of 40-bit WEP being most heavily used at doctoral-intensive institutions (39 percent versus 20 percent for everyone else). We found little difference between public and private institutions.

We noted that fewer than half of the institutions have installed wireless encryption/authentication, and a majority of institutions

Table 4-6. Status of Wireless Security

Wireless Security Technology	Adoption Stage (Percentage of Respondents)					
	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
Firewall	46.6	10.9	3.7	7.4	10.0	21.4
RADIUS	41.1	8.2	5.0	5.8	9.5	30.3
128-bit WEP	34.7	8.0	6.7	6.1	14.7	29.8
IP VPN	33.0	12.3	9.3	9.3	15.0	21.0
40-bit WEP	24.4	4.8	3.2	3.9	8.0	55.6
Vendor solution	18.5	4.0	4.3	3.1	8.9	61.2
Third-party hardware/software solution	17.6	5.6	6.3	4.7	10.7	55.2
EAP	14.8	7.2	7.2	9.3	21.7	39.7
Kerberos	12.2	4.1	6.3	4.4	16.6	56.6
AES	6.3	6.6	3.3	9.4	21.2	52.8

reported they are not considering implementing 40-bit WEP, vendor solutions, third-party hardware/software, Kerberos, or advanced encryption standard (AES). We also noted increased adoption of 128-bit WEP since the completion of the ECAR wireless survey in 2002. The data suggest that although clear standards have yet to emerge, institutions have deployed technologies to secure their wireless networks.

Rodney Peterson, EDUCAUSE security task force coordinator, found the above data to be disturbing. "It is remarkable that every approach is 'not being considered' by at least 20 percent or more of the institutions," he said. "This suggests to me that we need to take a fresh look at wireless security—problems and solutions—and develop an appropriate strategy for educational institutions. *The National Strategy to Secure Cyberspace* spent a considerable amount of effort discussing the importance of wireless security for federal government agencies. The results of the survey suggest that a significant amount of work remains for higher education, possibly including shifting views about the threats of wireless networks to an institution's overall security posture."

One explanation for the level of insecurity emerged in our interviews: numerous respondents said they were not quite sure what to do about wireless security because of what they considered to be either inadequate or inappropriate standards. They seemed to be waiting to see how things would fall out.

Authentication and Access Control

Access control is a set of procedures and processes performed by hardware, software, and administrators to monitor access, identify users requesting access,

record access attempts, and limit access to a system's resources to only authorized persons, programs, processes, or other systems. Authentication is a method for confirming a user's identification, often as a prerequisite to allowing access to system resources.

At an August 2002 National Science Foundation workshop in Chicago organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force, a select group of higher education IT security officers and technology architects recommended priorities for an action agenda on security tools. Highest on the agenda for authentication was a proposal requiring that every network connection on campus, including those in the library, be accountable to a specific person via authentication or some other mechanism. Further, two-factor authentication—the use of multiple forms of authentication such as a combination of a PIN and a one-time-use password generated by a hardware token—should be established where necessary. Such authentication is generally used to protect critical systems or those containing confidential data.

We asked the respondents what methods they used for authentication. Table 4-7 shows what is currently used, in progress, or being piloted. We also asked what methods they were or were not considering and why. The respondents most frequently mentioned the criticality of the data needing protection and ease of use.

We found that traditional, multiple-use passwords predominate, and passwords and PINs in general are the accepted methods. Sixty-five percent of institutions reported having a policy on passwords.

Passwords are problematic, however, as are many authentication tools. Andrew Conley, network security officer at South Dakota State University, noted that "fac-

Table 4-7. Status of Authentication

Authentication Technology	Adoption Stage (Percentage of Respondents)					
	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
Multiple-use passwords	72.9	7.3	0.5	1.2	5.1	13.0
Multilevel passwords	43.1	5.8	1.9	1.9	8.2	39.2
Password/PIN combination	40.2	5.6	1.3	3.8	15.9	33.3
Single-use passwords	39.2	6.1	2.8	3.0	11.1	37.3
Kerberos	22.0	4.2	3.9	3.9	14.1	51.8
PKI	9.8	5.8	8.2	5.6	28.6	41.9
Hard/soft tokens	8.1	2.2	3.3	3.1	17.2	66.1
Smart cards	7.0	3.6	5.2	2.3	27.6	54.2
Electronic signatures	6.7	5.2	9.3	8.0	32.0	38.9
Biometric technologies	1.1	0.5	4.0	0.3	18.2	75.9

ulty or staff write down passwords and put them on monitors or under keyboards, especially with harder passwords because it is difficult to remember them. We need to train and educate them better about such practices.”

We found that 22 percent of respondents used Kerberos. Of the institutions using Kerberos, 49 percent are doctoral institutions, followed by MA institutions (11 percent). Thirty-seven percent of all doctoral institutions surveyed use Kerberos. Paul Howell, information systems security officer at the University of Michigan, noted that his institution has deployed Kerberos, and many campus systems leverage the Kerberos infrastructure. “However, we buy

a lot of commercial software. Those products tend to know nothing about Kerberos. As a result, we have silo authentication schemes on campus.” Gregory Jackson, vice president and CIO at the University of Chicago, noted the “trade-off between the sophistication of a method and how broadly we can get it implemented. We’re going away from Kerberos (even though I think it’s a better method) to other forms of secure authentication such as SSH, SSL, or encrypted LDAP.”

More advanced tools such as PKI, tokens, smart cards, electronic signatures, and biometric technologies—user identification (and possibly access control) based on a physical, unchangeable characteristic such as a fingerprint, iris, face, voice, or handwrit-

ing—provide more reliable authentication but have low implementation rates. Most institutions are not considering tokens, smart cards, or biometric technologies.

Although institutions pursue different and multiple strategies, we did find that everyone uses something for authentication. As Figure 4-4 shows, 23 percent use only one form of authentication and 25 percent use two. But 42 percent use three or more forms of authentication, which stems in part from perceived levels of risk to particular information assets.

Choice of authentication methods is a policy decision at the University of Notre Dame. According to Gordon Wishon, CIO, associate vice president, and associate provost, the decision regarding when and where to use authentication is vetted with members of the university functional community. “We use an information security working group on campus with representatives from the student body, faculty, researchers, and

IT support people across the campus and members of the functional community,” he explained. “In terms of selecting technology for authentication—that is a responsibility of the chief technology officer, working with the engineering group and the chief security officer.” For the most part, respondents to our in-depth interviews told us that authentication method choice depends on the perceived sensitivity of the data being protected.

Terry Gray considers static authentication credentials (ID and password) one of the greatest security risks. “One of the first steps in securing a network computing environment is to make sure that authentication credentials are always encrypted en route, either via secure application/access protocols (SSH, SSL, or Kerberos) or via transport-level encryption (such as VPNs).” Clearly, higher education has some way to go to reach Gray’s recommended security level. Failure to adopt these tools is especially unfortunate

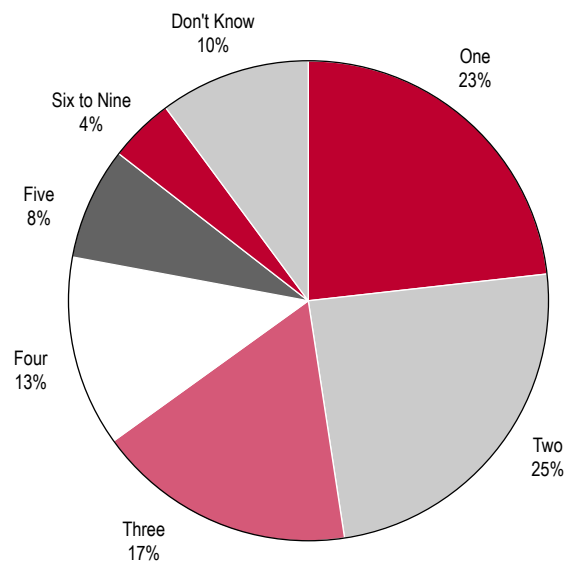


Figure 4-4.
Number of
Authentication
Tools in Use

because recent Web browsers support SSL, and no additional client-side software or configuration of clients is required to implement this form of session/path protection.

Looking at what institutions are doing by Carnegie class and in Canada (see Table 4-8), we not surprisingly find that doctoral institutions apparently have taken the lead—small as it may be—in using new technologies. When viewing by number of devices on campus, we found little difference except in Kerberos use at the doctoral and larger enrollment institutions.

We asked respondents whether their institution had a unified login or single-sign-on system and found that 19 percent had implemented such a system and another 19 percent were currently implementing single

sign-on. Forty-eight percent said they would implement such a system in the next two years; 14 percent said it was not under consideration. Doctoral institutions were more likely to have single sign-on in place. Of the institutions that had implemented a single-sign-on system, 43 percent had an enterprise directory.

Our findings closely track those of the 2002 KPMG study: the vast majority of their respondents (82 percent) still rely on user IDs and passwords. The survey’s researchers commented that the implementation of more robust forms of authentication has been slow and concluded that businesses have decided to accept the risk that tools such as biometrics could mitigate because of cost. The HIMSS respondents are much

Table 4-8. Status of Authentication, by Carnegie Class

Authentication Technology	Adoption, by Carnegie Class (Percentage of Respondents)								
	Overall	Dr. Ext.	Dr. Int.	MA	BA	AA	Specialized	System	Canada
Multiple-use passwords	72.9	76.6	74.3	71.6	65.9	63.3	74.5	58.8	76.2
Multilevel passwords	43.1	39.2	40.0	32.7	42.0	37.5	50.0	35.3	47.6
Password/PIN combination	40.2	41.3	40.0	47.2	3.2	27.1	34.5	27.8	47.6
Single-use passwords	39.2	30.2	41.2	41.5	37.3	36.7	37.7	29.4	33.3
Kerberos	22.3	43.4	22.9	15.0	12.3	12.2	11.1	27.8	14.3
PKI	9.8	9.5	11.4	7.4	11.1	2.0	11.1	11.8	9.5
Hard/soft tokens	8.1	18.9	5.7	4.7	0.0	0.0	13.0	6.3	19.0
Smart cards	7.0	6.8	5.7	8.5	9.9	2.0	3.7	0.0	0.0
Electronic signatures	6.7	9.5	8.6	3.8	7.4	0.0	9.1	5.9	6.2
Biometric technologies	1.1	1.4	2.9	0.0	1.2	0.0	1.9	1.0	4.8

heavier users of multilevel passwords, most likely attributable to the sensitivity of patient data.

As Table 4-9 shows, the 2003 CSI/FBI Computer Crime and Security Survey reported that 11 percent of their respondents have installed biometric tools versus 1 percent in our study. HIMSS noted that 8 percent of the health organizations used biometric technologies but also indicated that 60 percent of their respondents planned to use biometrics in the next two years. HIMSS reported that 18 percent currently use PKI and 40 percent planned to use it in the next two years, compared with 10 percent and 36 percent in our study.

Antivirus Protection

Ninety-seven percent of institutions surveyed have installed antivirus protection on their operating systems, 90 percent on their application servers, 92 percent on their e-mail servers, and 88 percent on other servers. Georgia State University conducted an antivirus audit by sampling PCs across

the university and found that they had 94 percent compliance. The overall figures compare favorably with the 99 percent finding of the 2003 CSI/FBI Computer Crime and Security Survey. Antivirus protection seems to go hand in hand with firewalls as a first line of defense, eliminating many worm and virus problems.

Sixty-eight percent of the institutions required that all institutionally owned systems have antivirus protection installed in order to be connected to the network, but only 36 percent required it of noninstitutionally owned systems. The requirement was weakest at large-enrollment and doctoral institutions. Baccalaureate institutions (87 percent) required it on institutionally owned operating systems, while only 30 percent of doctoral institutions required it. One factor that may explain the weaker requirements at large/doctoral institutions is the relative diversity of systems, some of which are not mainstream desktop systems with readily available antivirus solutions at competitive prices.

Table 4-9. Comparison of Authentication in Higher Education and Industry

Authentication Technology	Survey Population (Percentage of Respondents)			
	ECAR	FBI	HIMSS	KPMG
Multiple-use passwords	73	47		82
Multilevel passwords	43		82	
Password/PIN combination	40			
Single sign-on	19		14	
PKI	10		18	10
Electronic signatures	7		56	
Soft/hard tokens	8			19
Smart cards	7			10
Biometric technologies	1	11	8	2

Bruce Judd, associate vice president for university computing and telecommunications at San Jose State University, described his institution's efforts in this area. "We have distributed or optional desktop support on campus historically. Some areas—hundreds of computers—have no desktop support, no updates or patching. That was one of the reasons we had so many problems [in the past]. A significant portion of our campus does not have any antivirus software running. We installed e-mail relays with antivirus at the gateway and then, because we have 40-plus e-mail servers, we had to start insisting that people begin putting antivirus on their servers. We have a licensing strategy that allowed us to buy software for our systems by platform and distribute it to compatible servers across campus. Those two strategies—e-mail relay with e-mail antivirus filtering plus site licensing antivirus software with a fixed number of user seats—have solved a lot of problems, especially with e-mail viruses and worms."

Ninety-eight percent of the institutions had a site or volume license for antivirus

software, but only 55 percent of the licenses covered personally owned computers. The larger the institution, the more likely it was to provide a license for personally owned computers. Ninety-four percent of institutions with more than 25,000 enrolled students provided such licenses versus 37 percent of institutions with 2,000 or fewer enrolled students. According to Gregory Jackson at the University of Chicago, "We hand out antivirus software like candy."

In short, higher education is doing a good job installing and using antivirus software. But it appears that some institutions are reluctant to mandate usage, and some simply lack resources.

Strategies to Reduce IT Security Vulnerability

We asked institutions what strategies they were using to reduce IT security vulnerability, then rank ordered the strategies implemented. As Table 4-10 shows, strategies used most often include limiting protocols allowed through the firewall or router (76 percent), restricting or limiting access to

Table 4-10. Status of Strategies to Reduce IT Security Vulnerability

Security Strategy	Adoption Stage (Percentage of Respondents)					
	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
Limit types of protocols through firewall	75.8	10.3	2.4	4.3	2.4	4.8
Limit access to servers/applications	72.4	11.6	2.1	4.5	3.5	5.9
Timeout access	68.0	9.9	2.7	3.4	3.7	12.3
Recovery plan in case of disaster	48.5	31.4	2.6	7.6	7.4	2.6
Install closed desktop system	36.2	14.0	6.5	3.9	8.2	31.2
Limit URLs through firewall	30.5	7.5	4.6	3.1	6.3	47.9
Install directory inventory system to detect change	13.0	11.2	6.9	7.9	20.9	40.2
Use security devices for authentication	12.3	3.5	4.9	3.4	21.4	54.5

servers and applications (72 percent), and timing out access to applications after an idle period (68 percent). Little used were installing a directory inventory system to watch for undesired program changes (13 percent) and security devices for personal authentication (12 percent). The latter two strategies and limiting URLs through firewalls were not under consideration at almost half of the institutions. We found, however, that limiting URLs through firewalls was a strategy more often implemented at BA and MA institutions (33 percent) than at doctoral-extensive institutions (17 percent). Perhaps what is most disturbing in these data is that only 48.5 percent report having a disaster recovery plan.

Table 4-11 shows the strategies being used by institutions in different Carnegie

classes. Overall there is not much difference, but doctoral-intensive and baccalaureate institutions in general have implemented more strategies than the other classes have, and Canadian institutions have been more successful in limiting protocol types through firewalls (95 percent). The equipment installed also makes a difference. We noted earlier that 13 percent of the institutions had not installed firewalls. Therefore, we should see a proportionate use of limiting protocol types through firewalls.

With the exception of timing out access, the number of devices on the network does not seem to affect institutional strategies.

Summary of Findings

Higher education is adopting more technology to secure its information assets. But

Table 4-11. Strategies to Reduce IT Security Vulnerability, by Carnegie Class and Canada

Strategy	Adoption, by Carnegie Class (Percentage of Respondents)								
	Implemented (Overall)	Dr. Ext.	Dr. Int.	MA	BA	AA	Specialized	System	Canada
Limit types of protocols through firewall	75.8	59.2	82.9	73.1	81.2	64.0	89.1	68.4	95.2
Limit access to servers/applications	72.4	62.3	71.4	71.6	77.6	68.6	78.2	63.2	71.4
Timeout access	68.0	64.9	74.3	53.2	72.9	60.0	67.3	68.4	66.7
Recovery plan in case of disaster	48.5	50.0	54.3	45.9	54.1	35.3	41.8	52.6	33.6
Install closed desktop system	36.2	27.6	40.0	34.9	43.5	29.4	34.5	31.6	38.1
Limit URLs through firewall	30.5	17.6	20.0	28.7	32.9	33.3	43.6	33.3	38.1
Install directory inventory system to detect change	13.0	11.8	14.3	8.3	10.7	17.6	14.5	10.5	9.5
Use security devices for authentication	12.3	22.4	5.7	6.4	7.2	11.8	18.2	11.1	23.8

we found significant variations in adoption by institution size and type and between Carnegie categories. When compared with the private and business sectors, higher education lags in the installation of more advanced IT security technologies, but, as noted earlier, this may be due to different risk levels. We return to this topic in Chapter 10.

Endnotes

1. Institute for Information Infrastructure Protection (I3P), *National Information Infrastructure Protection Research and Development Agenda Initiative Report*, Version 1.0, 9 Sept. 2002, p. 23.
2. Shibboleth is a project of Internet2/MACE, <<http://shibboleth.internet2.edu/>>.
3. For a more detailed look at Gray's views, see his "Network Security Credo" at <<http://staff.washington.edu/gray/papers/credo.html>>.
4. The Computer Crime and Security Survey is conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad <<http://www.gocsi.com/press/20030528.jhtml>>. The survey, now in its eighth year, has the distinction of being the longest-running survey in the information security field. It is based on the responses of 530 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities.
5. Check Point, RSA, Symantec, and *Secure Computing Magazine* sponsored KPMG's 2002 Global Information Security Survey <<http://www.kpmg.com/microsite/informationsecurity/isssurvey.html>>. Telephone interviews were held with 641 senior managers responsible for information security worldwide.
6. J. Surmacz, "Most Security Experts Fear Cyber Attacks," CSO Online, 27 Feb. 2003, <<http://www.csoonline.com/metrics/viewmetric.cfm?id=509>>.