

6

IT Security Planning and Practice

*You cannot acquire experience by making experiments.
You cannot create experience. You must undergo it.*
—Albert Camus

In this chapter we address how the effective use of security technologies depends on information technology (IT) security practices. We pay particular attention to security planning, risk assessment, updating and maintaining systems, password use, monitoring, and the detection of threats. Installing technology is no guarantee that it will work; much depends on how, when, and where it is used, by whom, and with what level of effort and skill.

Security Planning

Institutions can be proactive or reactive with respect to security. One measure of a proactive security strategy is the preparation of an IT security plan that is comprehensive, in place, and followed.

We asked our respondents whether their institution had developed and adopted an IT security plan (see Figure 6-1). Thirteen percent reported that a comprehensive plan was in place at their institution; 10 percent said

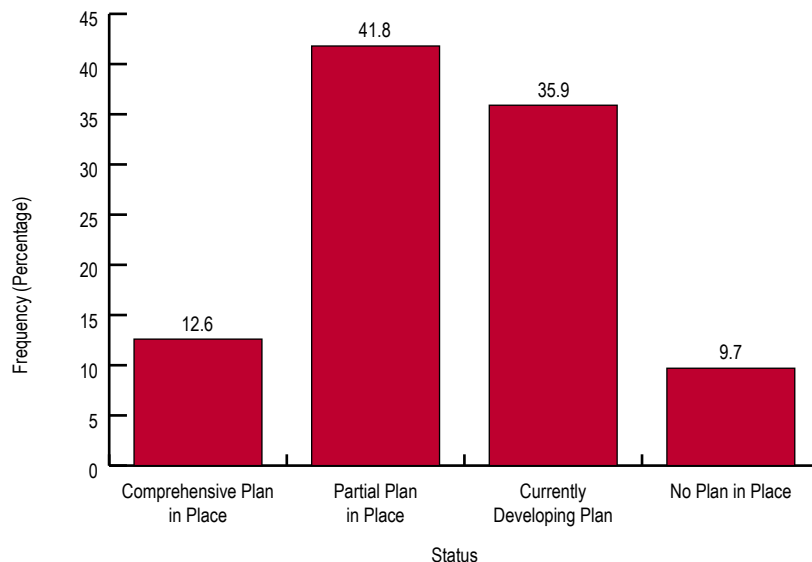


Figure 6-1.
Status of
Institutional IT
Security Plan

© 2003 EDUCAUSE. Reproduction by permission only.

no IT security plan was in place. Forty-two percent had a partial plan in place, while 36 percent were currently developing a plan.

Table 6-1 shows the breakdown by Carnegie class, which did not reveal much variation. Further analysis shows only minor differences in IT security plan adoption between large-enrollment and small-enrollment institutions. However, IT organization does have an impact. Where responsibility for IT security is spread across the institution, a security plan is less likely to be in place. More positively, institutions with a dedicated security staff will more likely have a plan in place. We return to the importance of this latter factor in Chapter 8.

Risk Assessments and Audits

A risk assessment helps an institution determine its security requirements. According to ISO/IEC 17799:2000, the risk assessment should estimate the harm to business likely to result from a security failure causing a loss of information confidentiality, integrity, or availability. It should also estimate the likelihood of a failure occurring given the current threat environment and the controls

currently in place at the institution. Periodic reviews are necessary to accommodate changes to the institution’s academic activities and business operations, to account for new threats and vulnerabilities, and to confirm that current controls are effective and operative. A risk assessment differs from a vulnerability assessment, which identifies errors or weaknesses in system design, implementation, or operation. A threat is an adversary motivated to exploit a system’s vulnerability and capable of doing so. In summary, risk refers to the likelihood that system vulnerabilities will be exploited or that a threat may become harmful.

Thirty percent of the institutions in our study had undertaken a risk assessment to determine their IT assets’ value and the risk to those assets (see Figure 6-2). We find this figure surprisingly low. Canadian institutions were more likely to have undertaken risk assessments (48 percent), followed by doctoral institutions (39 percent). Note, however, that 51 percent of institutions with a dedicated IT security staff have undertaken a risk assessment. These are most often doctoral-extensive institutions (see Figure 6-3).

Table 6-1. IT Security Plan Status, by Carnegie Class

Carnegie Class	Plan Status (Percentage of Respondents)				
	Comprehensive Plan in Place	Partial Plan in Place	Currently Developing Plan	No Plan in Place	Total
Dr. Ext.	14.3	50.6	31.2	3.9	100.0
Dr. Int.	11.4	54.3	31.4	2.9	100.0
MA	9.9	45.0	34.2	10.8	99.9
BA	15.1	34.9	33.7	16.3	100.0
AA	13.7	31.4	47.1	7.8	100.0
Specialized	12.5	35.7	37.5	14.3	100.0
System	10.5	42.1	47.4	0.0	100.0
Total	12.6	41.8	35.9	9.7	100.0

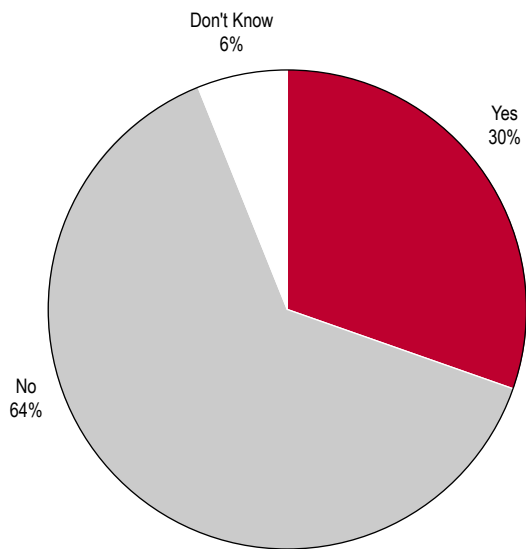


Figure 6-2.
Has an IT Security Risk Assessment Been Undertaken?

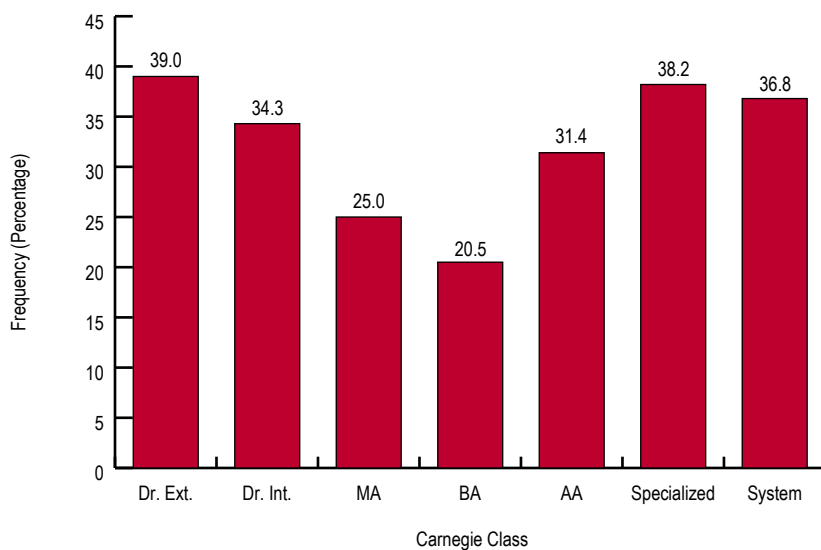


Figure 6-3.
Risk Assessment Undertaken, by Carnegie Class

We queried the periodicity of audits and vulnerability assessments and found that 9 percent perform IT security assessments monthly, 10 percent quarterly, and 26 percent annually. The rest responded “not regularly,” “never,” or “don’t know.” Again, doctoral-extensive institutions audited most often, usually on a monthly basis.

Also, we asked how often key enterprise systems and router configurations were audited to assess integrity and to look for unauthorized changes (see Figure 6-4). Forty-six percent audited on an irregular basis or not at all. Only 15 percent audited enterprise systems daily. These numbers appear to be surprisingly low, which suggests higher education has some work to do in the auditing area.

When we asked who conducted the reviews, 40 percent replied that an internal auditor conducted reviews; 55 percent used an external auditor, 22 percent used a vendor, and 35 percent used an external consultant. There was little difference by

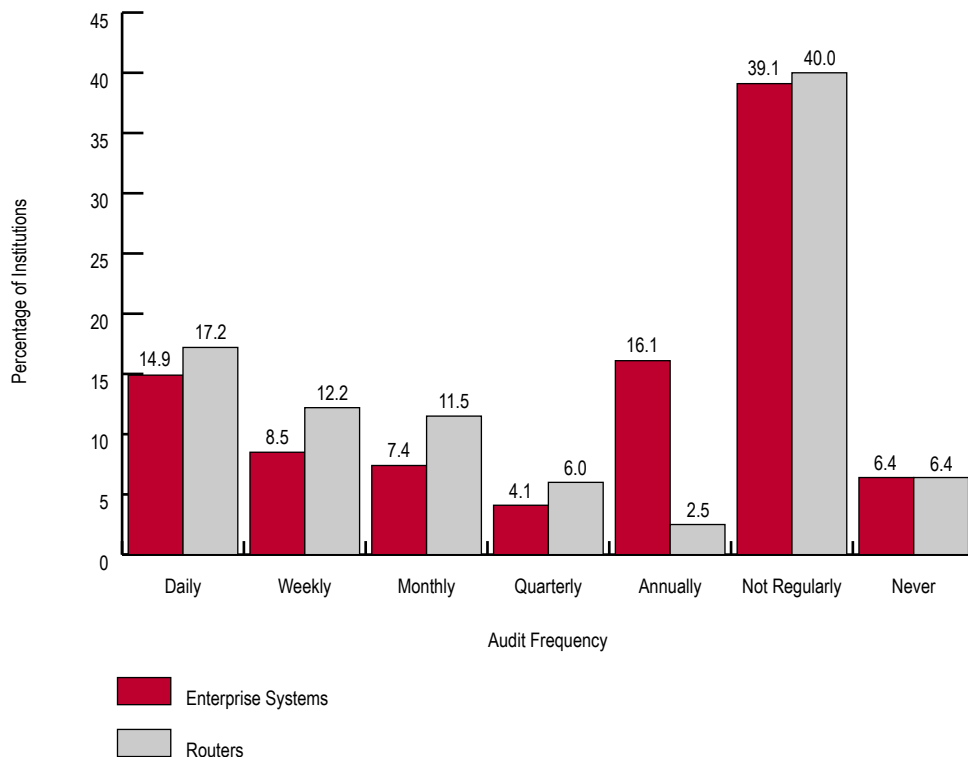
Carnegie class, size, country, and public versus private status in the use of vendors and external consultants. But doctoral and public institutions were by far most likely to use internal auditors and were also the largest employers of external auditors for this purpose.

Twenty percent of the institutions indicated that they had a risk assessment methodology for IT security. Only 12 percent of the institutions provided a guide or protocol for departments to conduct a self-assessment. Doctoral institutions were most likely to make a protocol available to departments, colleges, and business units.¹

Updating and Maintaining Systems

When asked whether their implementation protocol required all new enterprise systems and applications to be tested or certified for IT security, 48 percent of respondents said their institution required testing and 20 percent required certification. Public

Figure 6-4.
Audit Frequencies for Key Enterprise Systems and Router Configurations



institutions (60 percent) required testing and certification more than private institutions (40 percent).

It is important not only to update and maintain existing systems but also to build in appropriate security from the beginning. Jeffrey Savoy, information security officer at the University of Wisconsin–Madison, reflected on the importance of security being a part of system implementation. “We work to integrate security at the time systems are designed, developed, and implemented. It is critical. We bring the needed security expertise to the table. By involving security experts early in the system’s life, we can implement good security from the hardware up and can look at integration requirements from the beginning. Also, by seeking input from security experts early, a more accurate delivery date of the secure system can be obtained.”

Embry-Riddle Aeronautical University emphasized the importance of certification of their servers. According to Howard Muffler, chief security officer, “We certify our servers from the beginning—installed and prepared for whatever future action they are going to perform. They are certified along the way. They are also recertified from time to time,

although that is not a policy or procedure. We ensure that over time the system does not degrade as we upgrade applications and operating systems.”

The EDUCAUSE 2002 Core Data Service (CDS) survey asked institutions whether all critical systems were expeditiously patched or updated, and 82 percent of the 621 institutions surveyed indicated that they were. Figure 6-5 shows the findings by Carnegie class.

The ECAR survey asked a similar question: how many critical systems and applications are required to be patched or updated in an expeditious manner? Fifty-three percent said that all of their systems had such a requirement, 32 percent said most, 11 percent said some, and 1 percent said none. There was no variation among institutions by size, Carnegie class, public versus private status, or country. These data appear to corroborate the 2002 EDUCAUSE CDS survey findings.

Most respondents (62 percent) agreed or strongly agreed that they required all campus-owned computers connected to the network to have known security holes fixed. Fifty-nine percent agreed or strongly agreed that their institutions conducted regular and frequent scans to detect known

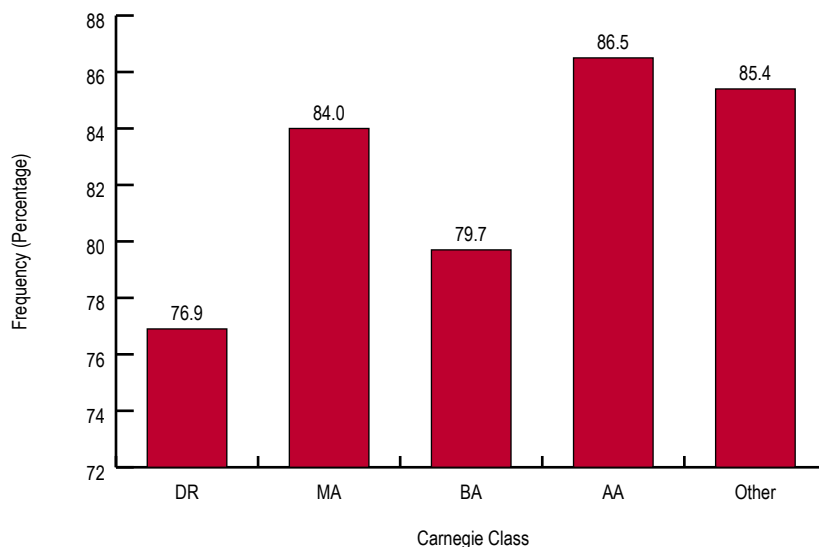


Figure 6-5. Respondents Indicating that Critical Systems Are Expeditiously Patched or Updated, by Carnegie Class

security exposures in critical systems. But only 40 percent agreed or strongly agreed that their institution conducted regular and frequent scans to detect known security exposures in all campus computers connected to the network.

We compared the means for the above three requirements and viewed differences by Carnegie class (see Table 6-2). The scale used was 1 to 5, with one being strongly agree and 5 being strongly disagree. We found little difference among Carnegie

class institutions with respect to both scanning questions, but we did see a negative progression from doctoral institutions (mean of 2.88) to associate's institutions (mean of 1.98) with respect to mandating that holes be fixed on institution-owned computers, perhaps indicating a lessened ability to mandate IT security behavior. This may well be because of the diversity and complexity of undertaking such a task at research universities. However, the proliferation of self-replicating worms like Blaster and SQL

Table 6-2. IT Security Practices

Carnegie Class		Require All Campus-Owned Computers Connected to Network to Have Known Security Holes Fixed	Conduct Regular and Frequent Scans to Detect Known Security Exposures in Critical Systems	Conduct Regular and Frequent Scans to Detect Known Security Exposures in All Campus-Owned Computers Connected to Network
Dr. Ext.	Mean	2.88	2.51	2.92
	Std. deviation	1.214	1.188	1.121
Dr. Int.	Mean	2.40	2.23	2.79
	Std. deviation	1.288	1.239	1.274
MA	Mean	2.34	2.47	3.07
	Std. deviation	1.181	1.106	1.139
BA	Mean	2.32	2.52	2.95
	Std. deviation	1.104	1.087	1.221
AA	Mean	1.98	2.18	2.67
	Std. deviation	1.010	1.014	1.088
Specialized	Mean	2.28	2.73	3.02
	Std. deviation	1.140	1.326	1.269
System	Mean	2.26	2.58	3.05
	Std. deviation	1.195	1.427	1.224
Total	Mean	2.38	2.47	2.95
	Std. deviation	1.179	1.166	1.177

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

Slammer may change all of this because such automated attacks do not focus only on large, well known targets.

Limiting and Controlling Access

In Chapter 4 we discussed access control 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. We noted also that traditional, multiple-use passwords predominate.

Changing Passwords

We asked institutions how often passwords were required to be changed (see Figure 6-6). Most respondents said 90 days or less (57 percent); 17 percent had no requirement. One baccalaureate institution required passwords to be changed daily. Table 6-3 shows common practice by Carnegie class.

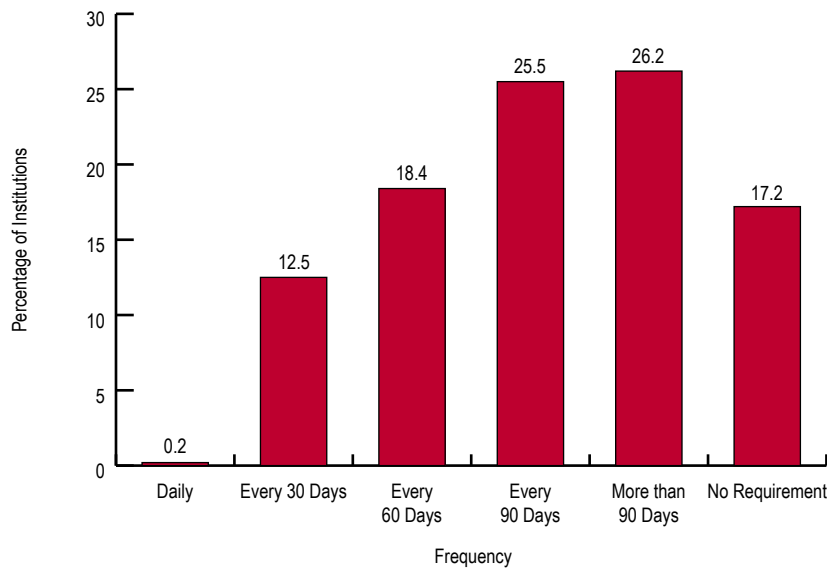


Figure 6-6. Password Change Frequency

Table 6-3. Password Change Frequency for Key Enterprise Systems, by Carnegie Class

Frequency	Carnegie Class (Percentage of Respondents)						
	Dr. Ext.	Dr. Int.	MA	BA	AA	Specialized	System
Every 30 days	7.9	20.0	11.0	9.5	13.7	16.4	10.5
Every 60 days	11.8	14.3	19.3	13.1	27.5	18.2	26.3
Every 90 days	17.1	22.9	33.9	28.6	15.7	20.0	15.8
More than 90 days	38.2	28.6	18.3	20.2	25.5	20.0	36.8
No requirement	21.1	11.4	13.8	23.8	9.8	16.4	5.3
Don't know	3.9	2.9	3.7	3.6	7.8	9.1	5.3

Eighty-eight percent felt that their procedures for identifying users before resetting passwords, tokens, and PINs were effective.

Eighty percent of the institutions provide individuals with only enough access to do their jobs. There were no significant differences found among Carnegie classes or by institution size, public or private status, or country.

Terminating Access

Institutions for the most part are good at terminating access when users leave the institution (see Table 6-4). All said that they routinely terminate access to enterprise systems. Some, like the University of Minnesota, Twin Cities, give students an e-mail address for life. The institution doesn't view termi-

nation as an end to all services and doesn't believe e-mail access to be as important a security risk as other types of access.

Background Investigations

We asked whether employees and contractors with key access to enterprise systems had undergone criminal background investigation and whether they were bonded. These are not commonly used practices in higher education—indeed, 67 percent did not investigate for criminal background of employees and 95 percent did not bond them. Eighty-five percent did not require criminal investigation of contractors, and 71 percent said “no” to bonding. There were no significant differences found by Carnegie class, size of institution, public or private status, or country.

Table 6-4. Access Termination

Processes and Practices	Percentage
Routinely terminate access to enterprise systems when users leave institution	100.0
Routinely terminate remote access when users leave institution	97.2
Routinely terminate e-mail access when users leave institution	96.4
Routinely terminate network access when users leave institution	94.1
Routinely terminate all access when users leave institution	90.7
Institution has procedure for identifying users before resetting passwords/tokens/PINs	84.9

Detection and Monitoring

According to the University of Washington's Terry Gray, the full spectrum of security embraces prevention, detection, and recovery. So far our focus has been on prevention. We now turn to detection and monitoring.

Monitoring User Accounts

We asked how often respondents' institutions audited user account activity to detect dormant, invalid, or misused accounts as well as to audit access control lists (see Figure 6-7). With the exception of access control lists, which doctoral-extensive institutions were most likely to audit daily, we found no significant differences by Carnegie class, size of institution, public or private status, or country.

Monitoring Networks, Operating and Enterprise Systems, and Routers

Monitoring unusual activity on the network is key to preventing problems. Terry Gray sees proactive vulnerability probing as one of the most important tools available to secure a population of computers. It can be done centrally or by individual departments. Like most aspects of security, it is not a one-time activity but requires an ongoing and recurring effort.

Our data show that two-thirds of respondents monitor their networks daily (see Figure 6-8). When combined with weekly monitoring, the cumulative percentage rises to 80 percent. Operating systems are monitored slightly less frequently. It is not surprising that network monitoring is somewhat more prevalent, as commercial tools to

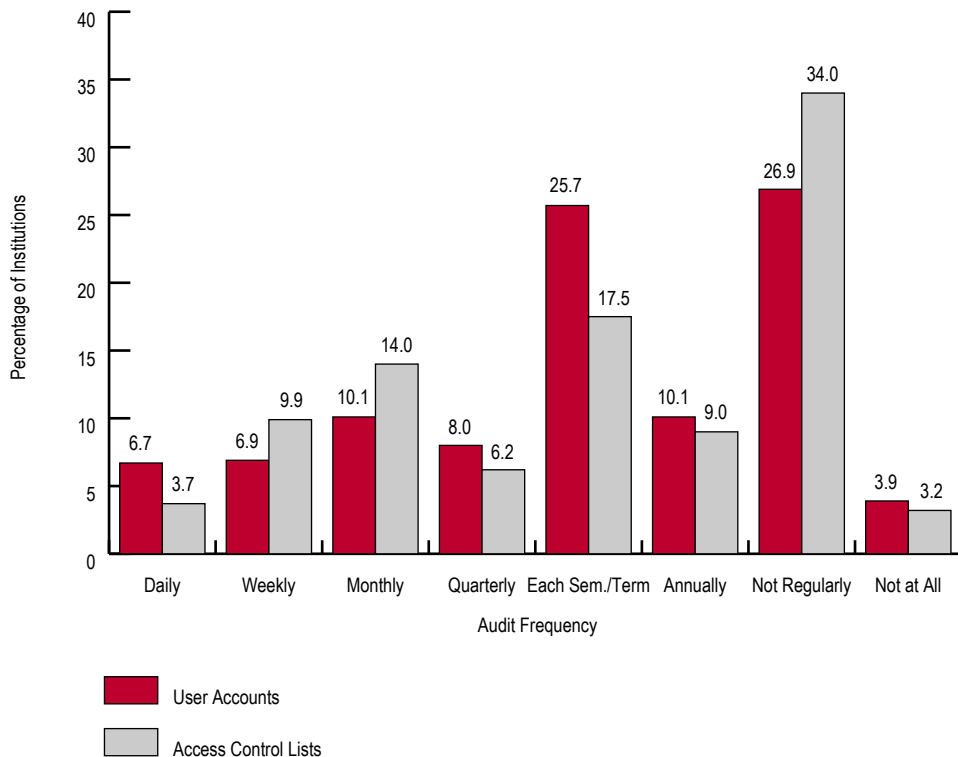
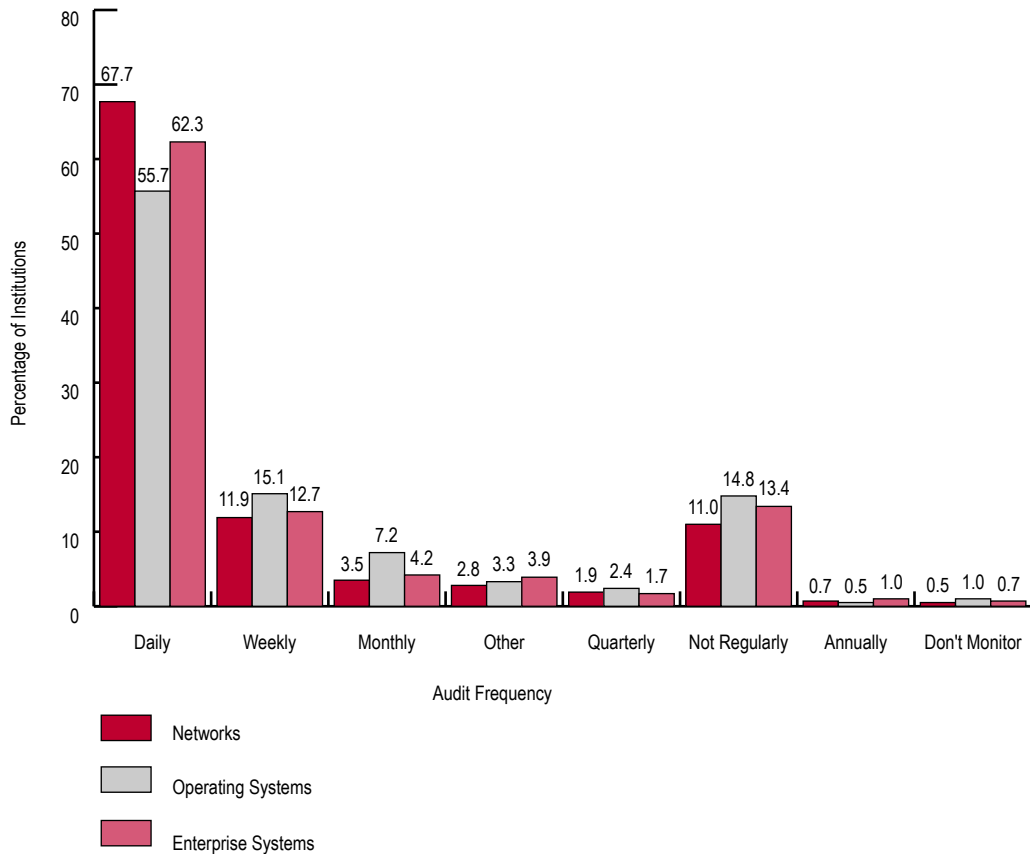


Figure 6-7. Audit Frequency to Detect Dormant, Invalid, or Misused Accounts and Access Control Lists

Figure 6-8.
Frequency of
Monitoring
Networks and
Core Systems



perform this task have been on the market for some time and are likely in use by many institutions' network operations groups. On the other hand, tools to monitor for operating system or application vulnerabilities are newer on the scene and may not yet be as commonplace in many institutions.

Most institutions monitor their networks, operating systems, and enterprise systems daily. Larger institutions (in terms of student enrollments) and doctoral institutions are more likely to monitor on a daily basis. Overall, Canadian institutions monitor their networks more frequently than do U.S. institutions.

Terry Gray considers traffic-level monitoring a more promising strategy than pervasive intrusion detection. He believes institutions need to implement tools that monitor net-

work traffic levels and send alerts when baseline thresholds are exceeded. With respect to intrusion detection, he said, "As network capacity and usage continue to escalate, it becomes increasingly difficult to believe that watching all network traffic for alarming patterns will prove to be a viable long-term solution. However, it may be reasonable to do for specific servers and can provide a validity check of whatever firewall rules may be in place."

Endnote

1. Available self-assessment guides include the *Security Self-Assessment Guide for Information Technology Systems* prepared by the National Institute of Standards and Technology (NIST). U.S. Department of Commerce, NIST Special Publication 800-26, Nov. 2001.