

## 8

# The Continuing Evolution of Effective IT Security Practices

*The art of living lies less in eliminating our troubles than growing with them.*

—Bernard Baruch

**K**ey to the importance and focus on IT security over the past 10 to 15 years is the movement of information systems from being a specialized tool used by a relatively small subset of higher education institutions to a critical system in the organism that is a modern college or university. Information security was once an afterthought on many campuses and in relation to most computer systems. Administrators chose to protect “critical” systems with encryption or other advanced techniques or to provide minimal protection such as antivirus software for the broader network. For the most part, security activities were reactive, focused primarily on countering targeted attacks by individual hackers or slow-spreading viruses replicated by individual users’ activities.

As use of the Internet grew beyond academia in the mid-1990s, the demand for connectivity grew, and colleges and universities, along with the rest of society, became ever more interconnected via the World Wide Web. Along with this increased connectivity came increased threats, as the proliferation of poorly protected systems connected to an open, public network provided hackers with a large number of easy targets, both through the traditional targeted attack as

well as through a new vehicle: worms that automatically propagated themselves to all unprotected systems. These worms primarily blocked network access by overloading the network, or they gave their creators access to the infected system to use it as part of a “bot-net,” or collection of compromised systems, to send spam, to launch additional attacks, or for other unsavory purposes. This was the scenario when ECAR conducted its initial study of information security in higher education in the spring and summer of 2003.

At that time, higher education was just starting to awaken to the paradigm shift caused by these new, automated attacks. When our survey research was conducted, in early spring 2003, there had not yet been many instances of automated attacks causing large-scale shutdown of institutional and corporate systems. This was reflected in our survey results, which demonstrated a purposefully limited use of protective technologies such as perimeter firewalls and a relatively low penetration of “soft” measures such as policies, awareness, and planning. As we conducted our detailed interviews in midsummer of that year, the SQL Slammer worm provided a new look at these emerging threats, shutting down numerous campus

networks by exploiting a known application vulnerability that many administrators had never patched.

By the time we had completed our research and presented our results at that fall's EDUCAUSE Annual Conference and ECAR Symposium, the discourse had shifted substantially. Earlier that fall, just as students were arriving on many campuses, the Blaster and Sobig worms hit, forcing IT organizations to clean the worms from thousands of PCs and causing many temporary network outages. As a result, many of the institutions and individuals who had earlier told us about the need to limit enterprise security measures indicated that they were rethinking their approaches in this new environment.

In the time between our previous study and this follow-up study three years later, we have indeed witnessed a marked change in the tools and techniques colleges and universities use to combat the ever-increasing wave of security threats facing them. Driven by the increasing frequency and virulence of attacks on their networks and systems, institutions have moved vigorously to secure their critical systems and protect their users. The degree of change in this relatively short time span is one of this study's key findings.

In many areas, our current study paints a brighter landscape. Use of many technologies has grown by double digits. Likewise, and even more encouraging, the adoption of soft IT security approaches has risen dramatically. However, despite the significant improvements discovered by our research, there is still considerable room for improvement. While we have indeed experienced impressive growth in the adoption of many important technologies and practices, many of these, including some that appear to have a significant impact on outcomes, are still not in use at 25 percent or more of our responding institutions. Moreover, our respondents indicated that while they are significantly more satisfied with the security of

their centrally controlled data, networks, and applications, their overall feeling of success actually fell since 2003.

This lower perception of success may relate to the changing threats our respondents are encountering. If, as described in the opening of this chapter, IT is seen as a critical system within the institutional organism—the circulatory system that moves the information that is increasingly the lifeblood of many organizations—the nature of attacks this system faces is changing for the worse. In computing's early days, attacks primarily focused on the organs constituting the system—the servers and computers connected to the network—most often with the goal of destroying them, using them to launch a subsequent attack on another machine, or occasionally targeting the data housed on them. Fighting off attacks against these organs was the primary goal at the time of our last study. Later, attacks were targeted at the arteries and veins connecting the organs—the network itself. Denial-of-service attacks, launched either from outside the network or by overloading the network using compromised machines within it, became a primary threat. This was the situation described immediately following our last study.

While both of these threats still exist today, security administrators have become adept at protecting key host systems and keeping the network running—hence, the increased perception of success in protecting centrally controlled assets. However, the new threat facing security administrators is targeting not the organs or veins of the system, but the blood itself: the data flowing through and housed on networks and computers, particularly personal data about the institution's constituents. These attacks can come in many forms, including keyboard sniffers installed to ferret out passwords, phishing attacks in which users are tricked into giving up personal data, compromise of improperly designed applications, or actual theft of physical as-

sets such as laptops or backup tapes housing valuable data. Such attacks differ from earlier ones in several ways. First, they often hit targets of opportunity—lightly protected systems or ignorant users outside the highly fortified areas of the organization. And perhaps more importantly, they are no longer just “nuisance” attacks that cause headaches for system administrators. These attacks directly target personal information for the purpose of theft and financial gain. This raises the stakes in the security game and requires different approaches to be successful.

Based on our findings, and in anticipation of the need for colleges and universities to continue to guard the assets of both the institution and its constituents in this changing environment, we suggest ways that higher education security practitioners can work to better protect assets beyond the walls of the data center. We elaborate on the changing environment and trends that can be reasonably ascertained from our research. On the basis of this data, we suggest effective practices and strategies that can help protect against today’s attacks and offer the flexibility to adapt to changing threats over time.

## State of the Practice

This section discusses the significance of this study’s findings and compares them, where possible, to those of the previous study. It shows the progress higher education has made in moving the state of the practice of information security forward and examines those areas where improvement is still required.

## Technology

As we expected, the events of late 2003 and the changes in the nature of threats seem to have driven many institutions to improve their defenses. Of particular note was the growth in the use of firewalls, which many institutions said they were not fond of in 2003.

In particular, the 22 percent growth in the use of perimeter firewalls in research universities since 2003 was interesting because many research institutions had ardently stated that perimeter firewalls would not be an effective solution in their environment when we spoke with them in 2003. Also significant was the growth in the use of interior firewalls—more than 27 percent across all Carnegie classes. Other rapidly growing technologies included virtual private networks, up more than 65 percent, and intrusion prevention systems, each up more than 30 percent. We also saw a 55 percent jump in the use of enterprise directories and nearly a 100 percent jump in the use of active filtering technologies. These statistics show that institutions have taken the threat of attack seriously and have taken steps to protect themselves.

While our statistics show that higher education has made significant progress in the use of security technologies, some areas could still be improved. Despite the high growth rates, fewer than half of the respondents to this survey were using intrusion prevention systems, 35 percent did not use interior firewalls, and nearly 25 percent did not have centralized data backup capabilities. Also telling was the lack of change in the authentication methods used by our respondents since 2003. Fully 95 percent of institutions reported still using traditional, weak username and password combinations. While almost 60 percent indicated they also use strong passwords within their organizations, only 27 percent were using Kerberos, and fewer than 10 percent reported the use of any multifactor authentication mechanism such as hardware tokens (SecureID), biometrics, or PKI. This is an area where higher education continues to lag broader industry benchmarks.

## Culture

In the 2003 study, we determined that our respondents were, as a whole, more focused

on technical solutions and put less emphasis on the “softer” aspects of IT security, such as planning, training, auditing, and codifying policies and procedures. We recommended that institutions seek out a more balanced approach, combining effective use of technologies with cultural solutions to more effectively combat threats.

We are happy to report significant progress on this front: The current study shows tremendous growth rates in the cultural aspects of security. Thirty-five percent of institutions now have a chief information security officer, up from 20 percent in 2003, and 62 percent of institutions now report having a centralized IT security function, up from only 39 percent in 2003. The growth rate of institutions offering IT security awareness programs jumped by 26.5 percent, with the largest reported program growth targeted at faculty. In the area of planning, we saw a huge change from 2003 to 2005, with a 49 percent rate of change in the number of institutions reporting either a partial or a complete security plan in place. We saw a 77 percent increase in the number of institutions that had conducted a risk assessment. We also found a substantial reported increase in senior management’s interest in IT security issues.

Despite the quantum leap forward in many of the cultural aspects of security, there is still room for improvement. For example, 58.7 percent of institutions formally designated a chief information security officer, and 37.0 percent do not have a centralized security function. These numbers may reflect limited resources or conscious policy decisions, but this topic warrants further study. While most respondents had some security policies and procedures in place, their coverage lacked uniformity: nearly 11 percent did not cover data backup, nearly 15 percent did not cover authentication and authorization, nearly 20 percent did not cover physical security, nearly 25 percent did not document individual employee responsibilities

for security, and more than 30 percent did not cover disaster recovery. More than 50 percent did not report having formal incident response procedures in place, nearly 50 percent don’t test new applications for security, and nearly 70 percent had not established security standards for application or system development. About 20 percent of respondents indicated they had no plan of any type in place for IT security. Fewer than 10 percent of respondents indicated they had undergone a comprehensive risk assessment in the last two years, and more than 40 percent still had not performed any type of risk assessment.

## Outcomes

On the whole, we found that respondents rated the success of their IT security programs lower in 2005 than in 2003, although they did rate some aspects of their programs more highly. Some key indicators, such as the barriers facing institutions as they deal with security, improved significantly. For example, 15 percent fewer institutions cited lack of awareness as an issue in 2005 than in 2003. Respondents offered a much higher assessment of the security of central applications, networks, and data than of those that are locally controlled.

We feel that several factors contribute to this lower rating of overall success. First, as described in the introduction to this chapter, is the changing nature of threats. As attacks target data rather than systems and networks, the defenses deployed to date are inadequate, as they generally are not as strong in the decentralized areas of the organization, where many new attacks are targeted. Also, institutions may have a greater awareness of the complexity of developing a comprehensive security program to combat these changing threats. Added to this is the complexity of managing security in the higher education environment, where many systems are not centrally controlled.

In the 2003 study, one of the key findings was that institutions needed to balance their use of technology with their use of cultural tools to better combat IT security threats. In this study, we certainly see that higher education made significant strides in this area, as well as in technical improvements, and that defenses are more robust than they were several years ago. However, the disparity in perceived security between central and local systems found in this study, along with the other areas highlighted as possibilities for improvement in this chapter, now put the spotlight on a new need: development of enterprise security programs designed to protect the entire institution—not just the central systems—in a coordinated, flexible manner. Several additional data points from the study support this need. Specifically, we found no change from 2003 to 2005 in the percentage of respondents who said that security practices were woven into the fabric of their institution (a low 34 percent), and only 25 percent of respondents agreed that security was part of the institutional employee culture in 2005. These points show that while significant progress has been made in implementing specific elements of a security program, these elements have not combined to produce enterprise-wide success.

## **Drivers of Change**

Developing an enterprise security program encompassing protection of both central and local assets is a large undertaking, particularly in the large, complex environment of a major university. Given that IT security, unlike most other major IT initiatives, does not provide visible or immediate benefit to institutional constituents, making the decision to expend scarce resources and significant political capital on such an endeavor requires a strong case.

## **Changing Nature of Threats**

One of the most compelling reasons to expand information security programs to

provide better coverage outside centrally controlled assets is the rapidly changing nature of threats. As highlighted in the introduction to this chapter, the target of many new attacks is no longer the operating system, the network, or control of the machine, but rather personal data on these systems' users and the organization's constituents. The driver of these hacking attempts is simple—profit. And the easiest way for a hacker to profit is not to steal top-secret research housed in a secure system or to attempt to access an organization's financial system and reroute funds. It is to find a weak link in the organization's security and use it to find personal data. With a relatively small set of information on an individual, a competent identity thief can open credit cards in someone else's name, empty a bank or investment account, or even take out a loan to buy a house or car. Information can also be easily sold to other identity thieves, generating revenue for hackers without directly linking them to the crime.

This change in hacking patterns was confirmed by Vincent Weafer, senior director at security vendor Symantec Corporation, in an interview with CNN in September 2005. Weafer said, "Attackers are increasingly seeking financial gain rather than mere notoriety. During the past year we have seen a significant decrease in the number of large-scale global virus outbreaks and, instead, are observing that attackers are moving towards smaller, more focused attacks" (Sieberg, 2005).

A number of extremely high profile cases of identity theft have recently been in the news. In early 2005, information surfaced on a successful theft of information on more than 140,000 consumers from ChoicePoint, a company specializing in identification and credential verification services. This theft was not carried out using traditional hacking means but rather by identity thieves who posed as customers of the business. The thieves were able to get access to people's names, ad-

dresses, Social Security numbers, and credit reports. The cost to ChoicePoint was high. According to a company statement (ChoicePoint, 2006), the firm had to pay \$15 million in penalties and agree to "Maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers," as well as "Obtain periodic assessments of the Company's information security program by a qualified, objective, independent third-party professional." These actual penalties were in addition to the huge amount of negative publicity the incident generated.

In another well-publicized incident in 2005, Bank of America lost backup tapes containing personal information on 1.2 million federal employees, including a number of U.S. senators. While there is no evidence that these tapes were used for illicit purposes, this incident highlights the need to look at security controls that go beyond protection of the machines in the data center to also look at processes and procedures.

In a similar incident in spring of 2006, the U.S. Department of Veterans Affairs lost information on 26.5 million current and former members of the U.S. military when a laptop computer containing the data was stolen from a data analyst's home. This incident highlights the need for strong policies, procedures, and enforcement, as one could question why this data was on a laptop in the first place, why it wasn't encrypted, why it was removed from a secure location, and why management was unaware this activity was taking place. It turns out in this case that the VA had policies on encryption and on removing sensitive data from facilities, but they were ignored. The data analyst lost his job over this incident, as did his supervisor and the undersecretary supervising the area. It will cost the VA upward of \$100 million to notify the affected veterans and provide them

with credit checking services (Greenemeier, 2006), and a lawsuit subsequently filed by a coalition of veterans' groups is seeking \$1,000 per affected individual, or up to \$26.5 billion, in damages (Keizer, 2006). If this lawsuit were ultimately to be successful, the precedent would be chilling for other organizations, such as colleges and universities, that are trusted with the personal information of others.

In all, more than 85 million Americans have had their personal data compromised since the ChoicePoint incident in February 2005, according to the nonprofit consumer information and advocacy organization Privacy Rights Clearinghouse. The group maintains a list of the incidents that constitute this figure on their Web site (Privacy Rights Clearinghouse, 2006). Of the 180 incidents listed between February 2005 and May 2006, 70, or 39 percent, occurred at colleges and universities.

Given the rising stakes owing to compromises of personal data, it is no surprise that this study found an increase in executive awareness. This increase should also extend to faculty, students, and staff who are all witness to the stories playing out almost daily in the media. These constituents expect that the institution will protect their personal information from exposure. The need to prevent such losses from institutional systems and networks is a new reality for higher education security administrators, one that requires an enterprise approach to information security. For example, it is easy to imagine an institution experiencing the same problem as the VA if a development officer loaded the institution's alumni database onto a laptop and lost it while on a fundraising trip, or if an institution lost credit card information stored not in the data center but on a weakly protected PC used to sell tickets in the athletics or drama department. Only a well-thought-out program that restricts the distribution of sensitive data, makes users aware of the risks, codifies appropriate policies and procedures, and provides the appropriate

tools, controls, and assessment mechanisms can significantly reduce risk to the institution from these types of threats.

## External Pressure

Pressure to improve security is not coming just from inside the institution in response to more malevolent threats. A number of existing and emerging policies and regulations from external entities also will affect institutions with regard to security.

One well-known type of legislation that increases the expense and exposure from potential security breaches is the notification law. Originally passed in California in 2003 and currently in place in at least 23 states (Hillebrand, 2006), such laws require organizations that may have inappropriately disclosed information on individuals in that state to notify them. While disclosure laws do not directly impact the practice of security administration, they do provide a case for making the changes necessary to prevent release of personal information, as each breach requires significant expense to determine whose information was compromised, how to contact each individual, and the actual cost of making contact and responding to the victims' concerns. This does not take into account the potential impact from loss of reputation. How likely are donors to give again if the university failed to protect their credit card number?

Another legislative topic that higher education information security administrators should be aware of is FISMA, the Federal Information Security Management Act, part of the E-Government Act of 2002. This legislation mandates compliance with a set of standards established by the federal government to ensure consistent application of effective security standards and practices.<sup>1</sup> Based on the act's definition of a federal information system as "an information system used or operated by an executive agency, by a contractor of an executive agency, or by

another organization on behalf of an executive agency," and driven by renewed focus on OMB A-123 (Rivlin, 1995), which holds federal executives responsible for instituting accountability and controls for assets under their management, some federal agencies are beginning to hold the recipients of their funds to the FISMA standards. For example, the Department of Labor has been auditing state agencies receiving their funds, such as unemployment insurance agencies, to ensure they have properly complied with FISMA. It is easy to see the Department of Education, the National Science Foundation, or the National Institutes of Health holding institutions receiving their financial aid funds or research grants similarly responsible in the future. Given this possibility, it makes sense for institutions to become familiar with the FISMA standards and to consider using these as a guide when developing their own security program.

Another federal mandate with similar impact could be Homeland Security Presidential Directive 12 (White House Office of the Press Secretary, 2004). HSPD-12 requires the use of more uniform, secure standards for issuing government identity credentials. Federal Information Processing Standard (FIPS) 201 (National Institute of Standards and Technology, 2006), issued by NIST, describes standards for the proposed Personal Identity Verification (PIV) system. HSPD-12 calls for these standards to be implemented by both federal offices and "contractors." If this terminology is interpreted to mean programs funded by federal dollars, colleges and universities also may have to comply. Institutions considering an identity management solution may wish to use this standard as a guide when looking at their own systems.

The Communications Assistance for Law Enforcement Act (CALEA) is another piece of federal legislation that may impact the technologies that colleges and universities deploy. CALEA requires facilities-based broad-

band Internet access providers, interpreted to include colleges and universities, to deploy standardized equipment and procedures to enable surveillance by law enforcement agencies. While specific technical requirements have not yet been issued, compliance with this particular legislation could be costly for institutions whose network infrastructure is not in compliance (EDUCAUSE, 2006) and could pose particular difficulties for institutions using VoIP on their networks (Bellovin et al., 2006).

Not all external mandates come from government agencies. Increasingly, other organizations with responsibility for personal information, such as financial institutions, are also mandating that their partners comply with certain security standards. For example, credit card giants Visa and MasterCard have teamed to create the Payment Card Industry (PCI) data security standard,<sup>2</sup> which requires all merchants offering payment with their credit cards to comply with their security standards (Visa Inc., 2004) and to prove compliance according to their published rules.<sup>3</sup> While the stringency of these requirements varies on the basis of transaction volume, they represent another trend that higher education security administrators must be aware of, and another tool that can be used to help design more effective security measures on campuses.

### **Developing an Enterprise Security Program**

To meet the institution's security needs in light of the threats and potential compliance challenges described above, institutions should consider developing an enterprise security program that addresses the needs of not only the institution's central organizations but also the broader campus community. This is not a matter of implementing new technology, providing better training, or hiring more security personnel, but rather developing

a programmatic approach to identify and protect key assets in an appropriate manner, wherever on campus they may reside, and to effectively react when a security incident does occur.

Implementing such a program in higher education is not easy. To get beyond the data center, where this study shows institutions are already doing a good job, to the distributed areas of campus, significant political will and capital will be required. Senior-level support will be needed to implement effective and enforceable policies and procedures and to develop effective governance for security efforts. However, the confluence of heightened awareness driven by high-profile incidents and the likelihood of regulatory mandates may make this the right time to successfully move such a program forward.

### **Defining an Enterprise Security Program**

An enterprise security program is a methodical, programmatic approach to implementing and managing security within an organization. The goal of such a program is to embed security into the organizational fabric, making it an accepted, ongoing part of everyday activities. It is not a security plan, which, although a component of the broader program, is generally focused on identifying and executing specific tasks. An effective IT security program incorporates several inter-related components, detailed below, that together help the institution meet its goals in a coordinated way.

#### **Governance**

One of the key components of an effective enterprise security program is the establishment of effective governance structures and processes. Like any IT initiative, a security program is much more likely to succeed if it is driven by the management and users of the organization, rather than by the IT

department. To be effective, the governance structure should include senior leadership, as well as representation from central departments, distributed users, and IT. The governance body should set the overall direction of the security program, guide and approve policy, and clearly support accountability and policy enforcement.

In addition to setting direction and providing guidance, the governance structure should serve as a clearly defined channel for decision making about IT security. Given the rapid decisions required in the face of an unforeseen threat or in responding to a security incident, having this formal structure for rapid resolution of issues is extremely valuable. Such a problem resolution mechanism is also key to addressing issues of perceived uniqueness among distributed users at larger institutions, who may be more likely to understand when a group of their peers asks them to comply with a standard than when such a request comes from IT.

### **Requirements**

Another critical and sometimes overlooked component of developing an enterprise security program is development and maintenance of a clear understanding of the organization's security requirements. This is critical to ensure that the right assets are being protected against the right threats.

One aspect of gathering requirements is determining what assets the institution has that require protection. These include servers, PCs, laptops, networks, applications, and other technical assets that one might normally consider. It also should include facilities, business processes, and personnel. Another critical component is to understand the institution's data, where it resides, and potentially why it resides there. This is absolutely critical to ensure the protection of constituents' personal information: Measures can't be taken to protect data if administra-

tors don't know it is there, as was evidenced by the VA incident described earlier in this chapter.

For development of a truly enterprise-wide security program, this inventory must include both central and distributed assets (although it can be conducted in stages). Creating and maintaining an asset inventory and a standardized, repeatable approach to assigning a security classification to those assets provides insight into the security measures required to protect them. FIPS 199 (National Institute of Standards and Technology, 2004) prescribes an approach for this type of classification.

Once the institution's assets are understood, another critical component of requirements gathering is the development of an organizational risk assessment. A risk assessment, using the approach shown in Figure 8-1, examines each major asset (or category of assets) as well as known vulnerabilities to determine for each:

- ◆ What is the likelihood that the asset will be compromised?
- ◆ What is the potential impact on the organization if the asset is compromised?

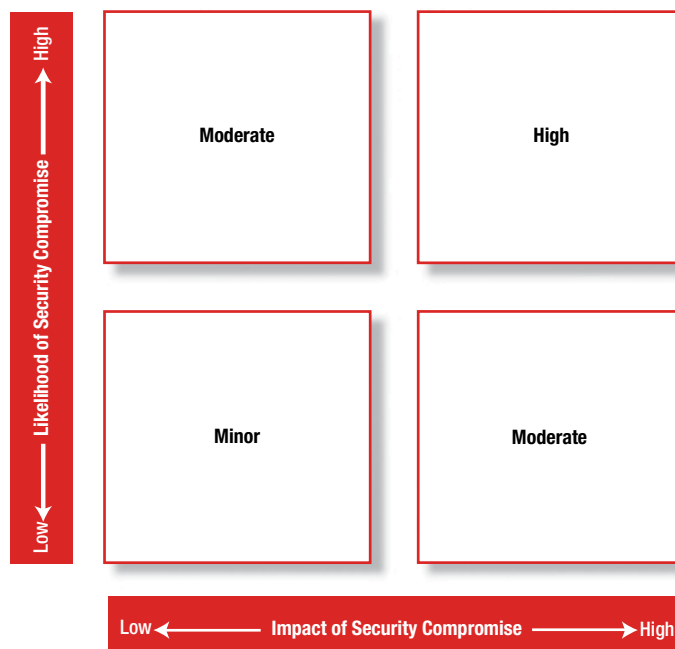
The results of the risk assessment guide the creation of the appropriate controls and protection mechanisms for the institution's assets, helping to ensure that the institution's limited resources are allocated according to real need.

### **Controls**

Based on the institution's requirements, the enterprise security program should include the development, deployment, and tuning of appropriate controls to protect its assets. Such controls will include the technical solutions already present at most institutions, although their deployment may be realigned on the basis of the risk assessment results, and other solutions may be added.

Controls must also include policies, standards, processes, and procedures that

**Figure 8-1.**  
Risk Assessment  
Matrix



guide the institution's personnel through security-related tasks such as testing new systems for security compliance, terminating an existing employee, responding to a security incident, or reporting a new asset that needs to be protected. Such procedural controls may vary in specificity, depending on their purpose and the people who will be affected. For example, the procedure for provisioning a new employee with network credentials may be very specific, as it would likely be an enterprise-level procedure. On the other hand, procedures for securely configuring a new server may be more general, as it is very likely that different parts of the institution would use different platforms, house different sorts of data, and so on. In this case, the purpose would be to ensure that a minimum standard is met, rather than requiring specific actions. Whenever possible, controls should be established in a consistent way that allows flexibility where needed, rather than developing specific controls for each slightly different scenario or part of the organization.

Another important aspect of controls involves establishing roles and responsibilities for the institution's constituents, along with clearly defined enforcement procedures if responsibilities are not met. For example, if an institution determines that it is the responsibility of each user of technology on campus to ensure that the system they are using meets the established minimum security standards, this responsibility needs to be clearly documented and communicated, and penalties for noncompliance should be clearly defined and backed by senior leadership.

### **Training**

Having an effective security program is impossible without the participation of the institution's faculty, students, and staff. As we reported in the 2003 study, most security incidents caused by internal users don't seem to be deliberate but rather are the result of ignorance or error. Many aspects of effective security management may seem intuitive to IT and security professionals, but they are not

at all part of the mindset of an accountant, an English professor, or a student.

Successful training, awareness, and communication programs can be developed in the same manner as controls—by looking at the risk assessment results and tailoring programs to meet each of the institution's needs in a logical way. There is no need, for example, to provide training on the secure handling of employee records to physical plant staff, whereas such training would be essential for HR personnel or department managers. Whenever possible, such training should be provided within the context of other employee training rather than as a technically focused, separate course. Technical training should of course still be offered for systems administrators and other IT professionals managing decentralized systems throughout the institution.

Communication, awareness, and training are critical components of the enterprise security program. They are the key vehicles for developing an understanding of the program among the institution's constituents and for refreshing them regularly on the program's details and importance.

### **Assessment**

It is not enough to develop and deploy security controls throughout the organization. To ensure that the institution's assets are as well protected as planned, it is imperative to develop the appropriate assessment mechanisms to periodically check for compliance with requirements. Such tools might take various forms, ranging from checklists that individuals or departments can use to make sure they have done the right things to automated testing tools configured to sweep the campus network and seek out poorly configured systems or applications. Institutions may wish to establish success criteria, such as compliance with security standards, and use them to measure their programs' effectiveness and identify areas where programs need to be strengthened.

### **Monitoring and Remediation**

Given the rapidly changing nature of information security threats, along with the continuous evolution of any organization, no security program can protect an organization without monitoring for noncompliance and changes and taking appropriate actions to remediate any issues that are found. Such monitoring should be done at several levels. First, organizations will likely determine that they need to perform continuous monitoring of their network against known threats, such as worm infections, unpatched systems, or patterns indicating an attack, and then take action for systems that have been compromised. Automated tools exist to help IT organizations perform such monitoring. At a minimum, organizations should perform a one-time assessment of each at-risk system as the program is implemented, to ensure it is adequately protected.

Another type of monitoring examines the compliance with and effectiveness of the security program components themselves. A periodic audit should be conducted for each program area to ensure it is operating as planned and is adequately protecting assets without excessively consuming resources or unnecessarily inconveniencing users. For example, an institution may wish to conduct an annual audit of the use of confidential information around the institution to ensure that it is still needed for a legitimate business purpose and is being adequately protected. A suggested approach is to examine one or two program components per month to ensure that the entire program can be kept up to date on a yearly basis without turning this review into a major initiative.

Finally, the enterprise risk profile should also be examined to ensure that the security program is still aligned to protect the correct assets. This should be done regularly. Additionally, the risk assessment should be updated whenever major changes occur in information systems or within the organization itself.

## Implementing an Enterprise Security Program in Higher Education

Managing IT security in higher education presents some unique challenges, especially at larger institutions that operate in a decentralized fashion. While the central IT department is expected to ensure the security of the institution's IT assets, it does not necessarily manage all of these assets. And, unlike in a corporate environment, these assets may be controlled by relatively autonomous faculty members, schools, or departments—or they may consist of students' personal equipment that isn't owned by the institution at all. This makes it difficult to implement one-size-fits-all solutions to many aspects of security. Approaches to creating an enterprise security program in higher education need to reflect this element of the institution's organization and culture.

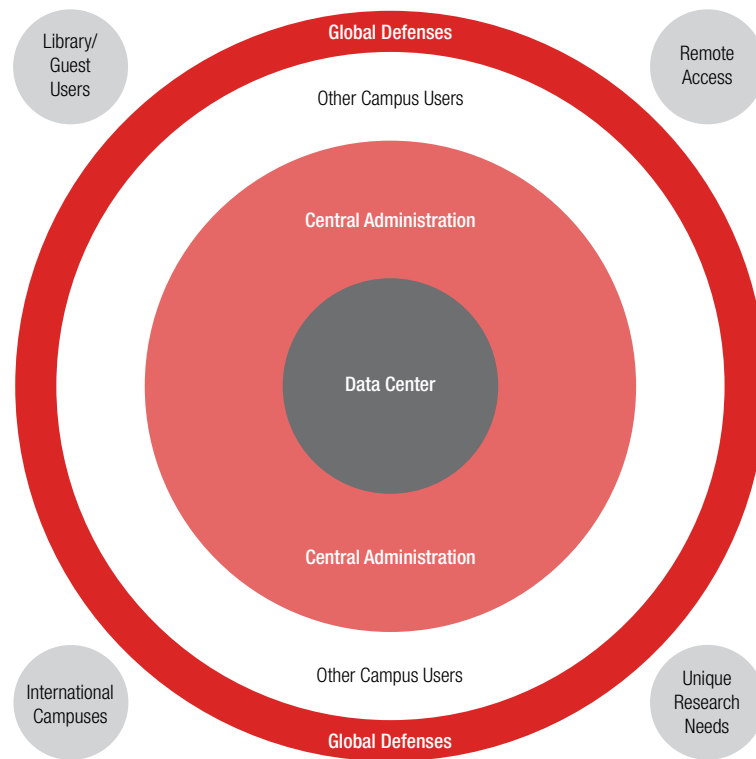
An enterprise security program for higher education should be

- ◆ *Standards based*, defining common standards that the institutional community will follow. This includes not only technical standards but also a set of policies and procedures that are accessible, understandable, actionable, and up to date.
- ◆ *Flexible*, to accommodate the diverse needs of the institution's distributed departments and user population.
- ◆ *Mission driven*, aligned to the organization's risk profile and developed through the participation of a broad governance body. It will be difficult to succeed with an IT-driven program.
- ◆ *Adaptable*, designed around principles and risk profiles, not specific threats or systems. This will allow it to change as the institution changes and as new threats emerge.
- ◆ *Simple*, for individuals and departments to implement, in order to gain their willing participation. This may require significant work on the back end by IT to deliver this level of performance.

- ◆ *Measurable*, with metrics established to gauge the program's performance so it can continue to be improved in a meaningful way.

Failure to recognize the unique aspects of the higher education environment when designing security programs can lead to less than optimal results, as institutions may either cater to the lowest common denominator ("we don't know what services the faculty will need, so we won't configure our firewall to block anything") or be overly controlling ("we'll require all users to have IT scan their machine before connecting it to the network"). A common reaction when an organization discovers it needs to make itself more secure is to attempt to consolidate control in order to obtain direct management of the assets to be protected. While this approach can be successful at some (mostly small) institutions, it will often lead to users' taking steps to bypass the mechanisms put in place, which they view as either additional bureaucracy or a power grab by IT. To avoid this pitfall, institutions should consider approaches that respect the differences among the various constituencies that make up the institution and tailor approaches based on the degree of control IT has over the assets in question. Figure 8-2 illustrates this concept of "zones of control."

The concentric circles represent the various constituencies that make up a typical institutional community, grouped by the level of control IT can reasonably expect to exert over how that constituency approaches IT security. The red circle around the outside represents the global security measures put in place, such as a perimeter firewall, enterprise antivirus protection, and intrusion detection tools, that equally protect all of the institution's assets. The circles around the outside of the diagram represent examples of special situations that IT may need to deal with on an individual basis.



**Figure 8-2.**  
**Zones of Control**

- ◆ **Zone 1: Data Center.** At the center of the diagram is the data center, an area totally under IT department control. For IT assets in this zone, IT can set policies, procedures, and access restrictions; mandate the use of specific security technologies; and even manage the assets' physical security. This zone is also among the most crucial to protect, as it contains many of the institution's mission-critical services and houses much of the institution's confidential data. The institution's network infrastructure would also likely be included in this zone, even though not all components are physically housed in the data center itself.
- ◆ **Zone 2: Central Administration.** The next zone represents the IT assets being used by employees of the institution's central administration. While IT may not have complete control over the machines in this zone, it can work with the institution's management to implement specific controls needed to ensure these assets' protection. Also, since central IT will likely support the assets used within central administration, it can ensure that systems are configured properly and are running appropriate security tools. Protection of assets in this zone is important, as these employees are likely to be working with sensitive data. Note that institutions may wish to separate out auxiliary services (such as facilities and student housing) as a separate zone, because governance and support of these areas sometimes varies significantly from the approaches used for administrative departments like finance or human resources.
- ◆ **Zone 3: Other Campus Users.** The outermost zone represents IT assets on campus not under the control of either IT or the central administration. This includes

machines owned by individual schools, departments, and researchers, as well as student-owned systems. (Institutions may consider splitting these constituencies into multiple zones if approaches vary significantly.) For IT assets that fall into this category, a persuasive rather than a coercive approach is likely to be more successful. Use of awareness and training activities, implementation of clear, flexible policies and procedures, and provision of necessary resources such as antivirus software and interior or application firewalls will go a long way toward protecting the assets in this zone without requiring direct action by central IT. This will leave these users with the flexibility to adapt the security measures they take to meet their specific requirements. IT organizations may also offer incentives to users to host their sensitive systems in the central data center, providing higher levels of protection for these assets.

We find an example of how this approach may help make an institution more secure in the area of authentication. In Chapter 3, we saw little change from our previous study to this one in the way institutions authenticated their users, and use of multifactor authentication is still limited. This is an area where higher education lags broader cross-industry benchmarks. One reason higher education may not implement more secure multifactor approaches is the decentralized nature of the organization. Implementing such solutions requires purchase and distribution of hardware and software components, training, and user support. Many institutions are understandably reluctant to do this for a broad population of users—many of whom are not employees—using a wide range of platforms to access multiple systems. Providing fingerprint readers to enable biometric authentication, for example, would be impractical across the institution.

However, using the zones approach as part of a broader enterprise security program, an institution would look at its assets, establish the risk profile of each, and determine where more stringent authentication methods might be necessary. In this case, the institution might install biometric access for their system administrators to access the data center and critical enterprise systems, issue hardware tokens such as SecureID to administrative users with access to sensitive data, and continue to use strong username/password authentication for the broader student and faculty population. Individual departments and users should be able to request the use of one of the stronger authentication methods should they feel that their situation warrants it, and IT should have mechanisms in place to support this use.

The zones approach can also serve as a guide for implementation efforts. Begin by protecting the areas where a direct impact can quickly be made, then expand efforts outward, making the institution more secure with each pass.

## Steps to Implementing an Enterprise Security Program

For institutions interested in moving forward with developing an enterprise security program, we highlight some critical steps below.

- ◆ *Secure senior management support.* Moving security management to an enterprise level will require the political support of the institution's senior leadership. This will be critical to give credibility to the program and the governance structure designed to manage it, as well as to ensure that the controls and enforcement procedures implemented have teeth. Given the heightened awareness of the consequences of security failures, it should be easier to make this case at most institutions today than it might have been in the past.

- ◆ *Implement governance structure.* Because most institutions don't operate in a top-down fashion, implementing a governance structure representative of the campus community may be just as important to success as securing executive support. Governance teams should be small enough to be able to effectively and rapidly make decisions, yet diverse enough to incorporate the viewpoints of different types of campus constituents. A multitiered structure—for example, executive and operational—may help achieve this goal.
- ◆ *Communicate.* Clear, frequent communications are essential to any change initiative. Whether through formal training and awareness programs or just through e-mail updates, members of the campus community should be kept aware of changes being made and of their roles in the vision.
- ◆ *Develop inventory.* Institutions must identify and classify their assets that require protection. This is extremely critical for data, as, ultimately, this is what we are trying to protect. Classification can be simple—for example, (1) Regulatory Compliance: Needs to be protected due to legislation or other regulation; (2) Confidential: Institution has determined that this data should be protected; (3) Internal: Open for use by internal users but not for public consumption; (4) Public: No protection needed, though a more complex classification could be used if deemed necessary.
- ◆ *Perform risk assessment.* Examine institutional assets to determine the level of protection they require and develop a risk mitigation plan to address risks with an appropriate level of response.
- ◆ *Implement controls.* On the basis of the risk assessment, implement needed technical, procedural, and organizational components. Develop approaches to

accommodate the needs of the broader organization, per the “zones of control” approach described above. It may be necessary to provide central support for some distributed areas with special needs.

- ◆ *Monitor and refine.* Develop and implement monitoring capabilities and procedures for both the IT assets and the program itself. Conduct periodic monitoring that aligns to the risk profile of the asset in question. Use the monitoring results to improve and tailor the program to more effectively meet the institution's needs.

## Conclusion

The increasingly high profile of information security incidents has raised awareness of the importance of effective security management. The good news is that institutional users are much more likely to understand the need for strong security measures and thus will be more willing to participate in such efforts than they were even a few years ago. However, this awareness also will shine a harsh light on the institution's security activities, as user demands will continue to rise and tolerance for failure, given the increased stakes, will fall.

Given this change in user perceptions, combined with the rapidly changing nature of threats, having a true security program consisting of technologies, processes, and human components aligned to the institution's risk profile, and flexible enough to work within a decentralized higher education environment, will allow institutions to more easily adapt to new threats as they emerge, rather than targeting specific threats with specific measures. Although instituting such a program will be difficult, it is nevertheless the step needed to move security management to the next level and continue to provide a secure teaching, research, and business environment for our constituents.

## Endnotes

1. FISMA standards can be found in the NIST publications located at <http://csrc.nist.gov/publications/index.html>.
2. Information on the PCI standards is available from [http://usa.visa.com/business/accepting\\_visa/ops\\_risk\\_management/cisp.html](http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html).
3. PCI merchant rules are available from [http://usa.visa.com/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_merchants.html](http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html).