

## 9

# Effective Practices and Lessons Learned

*People seldom improve when they have no other model but themselves to copy after.*  
—Oliver Goldsmith

Chapters 4 through 7 described the current state of information technology (IT) security at 435 higher education institutions. In Chapter 8, we analyzed both quantitative and qualitative data to identify factors that appear to affect institutions' security outcomes. In this chapter, we synthesize what lessons we have learned about the practice of IT security in higher education. A key advantage to surveying hundreds of institutions on IT security is the opportunity to assess what went well and what could have been done better, thereby enabling us to provide valuable insights for the rest of the higher education community. To quote Oscar Wilde, "The only thing to do with good advice is pass it on. It is never of any use to oneself."

Several common themes emerged from our survey data and in-person interviews concerning effective ways to improve institutional IT security. While many of these insights might sound familiar, their recurrence underscores the importance of incorporating them into our collective thinking about how best to structure and execute IT security activities on our campuses. We recognize that cultures, resources, and technical

environments vary significantly across the institutions surveyed in this study and that no single practice described here will necessarily work everywhere. Our data underscore the diversity of our campuses.

## **IT Security Is Not Just About Technology**

While deploying technology is necessary to achieve effective IT security, institutions must place equal if not greater weight on the "soft" aspects of security, including ongoing user awareness; creation of effective, understandable, and enforceable IT security policies; and effective communications, both with the end-user community and within IT organizations. Without such measures, organizations could invest large amounts of money in the latest and greatest technologies but still experience a security breach when users unknowingly employ a weak password, store confidential information on an insecure system, or ignore security policies they don't understand or consider troublesome.

As indicated in Chapter 5, most respondents in our survey agree or strongly agree that IT security problems inadver-

tently caused by authorized users are a significant concern. Despite this, nearly two-thirds of the institutions do not have formal awareness programs in place for their faculty, students, and staff. However, in Chapter 8 we showed that universities with awareness programs in place feel more secure than those without such programs. Likewise, Chapter 8 showed us that institutions with formal IT security policies ranked their security programs' success higher than those without.

These data indicate that nontechnical aspects of IT security can play an important role in enhancing the effectiveness of an institution's IT security program. As James Bruce, vice president for information systems at the Massachusetts Institute of Technology, stated regarding security awareness and regulations such as FERPA, "People don't have trouble with the security. They have trouble understanding the rules that mandate the security and how they are applied." This view is echoed by numerous other IT security practitioners we interviewed.

Gordon Wishon, chief information officer at Notre Dame University, suggested, "Commit resources not only to technology solutions, but to education and awareness—particularly education and awareness among students and faculty and certainly staff, too." Andrew Conley, network security officer at South Dakota State University, agreed. "You can put all the technology in place, but if you don't let the users know, a lot of times they can find ways around it or they may do 'bad' things unknowingly. User awareness is one of the areas that really needs to be addressed in the security realm." Jeffrey Savoy, information security officer at the University of Wisconsin–Madison, emphasized, "Your end users are your best firewall. It's important to get their buy-in on good security practices. They can do important things such as using good pass-

words, updating operating systems, keeping virus definitions updated, and not knowingly circumventing existing security controls."

Morrow Long, director for information security, Yale University, explained, "Much of your job is not technology and technical. It is people based—working with people, talking to people, dealing with people problems. The most important thing is to communicate well with people. They want to understand what you are saying; if you talk to them in technical jargon, they won't understand you." Larry Lidz, senior network security officer at the University of Chicago, said, "There are two main things: convince everyone that security is something they should be concerned about, and build up trust [among the user community]." And according to Beth Cate, associate university counsel at Indiana University, "The more educated Indiana University personnel are concerning security issues and the tools at hand, and ways to minimize risks, the better off we will be."

## **IT Security Requires Senior Leaders' Engagement**

Involvement of the institution's senior leadership with IT security is important to the security program's success. It is difficult to create comprehensive programs and enforce IT security policies without senior academic and business officers' involvement and support. And it is difficult to convince the university community to conform to those policies without senior leadership's practicing the policies and articulating the importance of the issues. The institution's IT security culture needs to change, and that requires the active engagement of the senior academic leadership and faculty governance.

In Chapter 5, we learned that, on average, senior executives are not as involved

in the development of IT security policies as the technology management and staff. However, the analysis presented in Chapter 8 indicated that at institutions where the president or provost was involved in developing IT security policies, respondents felt that their IT security efforts were significantly more successful. Eric Cosens, information systems auditor at Indiana University, explained, "It all starts with the tone at the top. The CIO and campus administration here have made security a priority. The proper tone at the top makes what we do more effective. It is the foundation of the control structure; otherwise, policies are seen as optional and not taken seriously. It has to become part of the institutional culture."

Engaged and informed senior leadership is also a prerequisite for funding. In Chapter 5, we discovered that 75 percent of institutions considered IT security one of the top three institutional priorities. Nevertheless, we also observed that only 28 percent of institutions agreed or strongly agreed that their institutions were providing the necessary resources to address IT security issues, and 63 percent expected no increase in their staffing levels for IT security, while 17 percent expected a decline. Similarly, more than 50 percent of respondents expect their spending on security hardware and software to decline over the next year.

A significant dichotomy exists between the perceived importance of IT security at institutions and the resources being made available for executing IT security initiatives. One major factor that apparently contributes to this imbalance is the difficulty of engaging an institution's senior leadership in discussions about IT security and its importance. Chapter 5 showed us that only 11 percent of institutions "often" discuss IT security at senior-level cabinet meetings, and only

17 percent report on IT security "often" to senior management. Because it is often difficult to see whether IT security is working well unless a significant incident occurs, senior management might feel that IT security at their institution is being handled adequately, while those responsible for security struggle to find the necessary resources to protect the institution. Making senior administrators aware of the need for IT security and the issues the institution faces day to day is critical for ensuring that security will be treated as a serious issue—and for getting appropriate levels of funding. This point of view is shared by several of the practitioners interviewed.

"We need to pay more attention to politics," said Robert Mahoney, team leader for network security at MIT. "In general, the notice of IT security is by its failure, or by some draconian measure that is taken. If you are not maintaining good relationships [with upper management], the only time the word 'security' comes up at the highest levels is as a problem."

Bruce Judd, associate vice president for university computing and telecommunications, San Jose State University, said, "Because I have kept the president's cabinet as well as the academic senate budget committee apprised with periodic reports on network security and security issues, they now have a greater appreciation of the importance of network security. They raised security funding up to the mission-critical [level], whereas before it was viewed as just an option. Now it has the same criticality as the telephone system, the power plant; it is viewed as a utility. I had to do a lot of outreach by laying out the facts and saying things like, there were 280,000 attempts in the last three months to get into our system."

## IT Security Requires Effective Planning

In Chapter 6 we noted that 13 percent of institutions reported having a comprehensive IT security plan in place. Forty-two percent had a partial plan in place, 36 percent were currently developing a plan, and 10 percent had no plan at all. IT security threats are continuously changing, and institutions need to be prepared to react to a myriad of new threats as they emerge.

William Paraska, director of university computing and communications systems at Georgia State University, illustrated this point: “You have to have a plan—you have to know what’s out there, what’s going to happen to you, and how you’re going to deal with it. Some schools are out there floundering—without an overall approach [to IT security].” Michael Adelaine, chief information technology officer at South Dakota State University, espoused a similar approach. “We’re trying to be much more proactive than reactive. We’ve sent out a lot more ‘feelers’—trying to look in those dark, deep Web sites where chats occur to get a sense of the drumbeat that goes on out there. We set up a plan as to how we were going to deal with a potential cyber attack. We have firewalls and a whole host of systems there. But as far as the human element, we’re out scouting the territory to see if there is trouble on the horizon, where it might affect us, and then we develop a plan. Before, we just hoped our technologies were in place.”

Jeffrey Schiller, network manager at MIT, gave a more concrete example of how effective incident response procedures can impact an institution’s ability to react to a new threat. “We have a very effective incident response team. The fact that we can say we had zero to one Code Red [worm] infections on a campus this size [shows the

importance of a strong incident management capability].”

## IT Security Requires Diligent Monitoring

We cannot overemphasize the importance of monitoring institutional networks and systems for abnormal activity. Regular monitoring for abnormal activity helps institutions quickly identify incoming attacks, locate and isolate machines with known vulnerabilities, or react to security breaches in process, such as a PC infected with a worm. On the basis of our survey research, higher education appears to be doing a relatively good job of monitoring its systems. Sixty-six percent of respondents indicated that they monitor their networks daily, 54 percent monitor their operating systems daily, and 59 percent monitor their enterprise systems daily. Fewer than 15 percent of respondents indicated that they do not monitor these components regularly. However, only 58 percent of respondents indicated that they conduct regular and frequent scans to detect known security exposures in their critical systems, and only 39 percent agree that they conduct such scans for all university-owned systems connected to their networks. Our respondents described several different monitoring approaches.

Philip Long of Yale University said, “We license the ISS scanning system and do a campus-wide scan of all campus computers for vulnerabilities on a periodic basis. We collect them in ways that make sense and forward them to the systems’ administrators of record—for those systems for which we have records. That is actually quite an educational experience for those people. Our security team is called from time to time to do security assessments of various kinds of systems; we will run the scans on the system and give advice for free. We will

not remediate for free; we are a charge-back operation.”

According to San Jose State’s Bruce Judd, “A lot of the monitoring tools we use are not expensive, as they are open-source tools. We take advantage of open-source tools, so the cost of what we implement is really the cost of the hardware, not the cost of software and software maintenance. There are some wonderful open-source tools: Big Brother and Cricket, for example. It is acceptable to use open-source tools for monitoring.”

MIT’s Robert Mahoney described a different approach to intrusion detection. MIT runs an open network without a perimeter firewall. This causes a problem, since “a lot of [intrusion-detection systems] products assume you are behind a firewall, and so, if you see something, it has penetrated your firewall and must be important.” MIT’s approach is to “mostly focus on outgoing attacks, which either represent a compromised machine or malicious behavior, and we rarely see a malicious attack [originating from here].”

### **Work With, Not Against, Your Constituents**

In academic environments, particularly large research institutions, many constituent groups on campus often suspiciously view the IT security team as “Big Brother.” This perception is sometimes enhanced when institutions take an overly aggressive posture toward enforcing campus policies, thereby encouraging people or departments to find workarounds rather than comply. MIT has shared some interesting techniques for working with its campus communities to enhance security compliance.

MIT has developed a sense of community around IT security by creating a virtual IT security team staffed by two central IT full-time employees but also enlisting volunteer participation from nearly every school and

major research laboratory on campus. By allowing and encouraging broad participation in IT security efforts, MIT gains consensus for broad-reaching IT security decisions while leaving each unit enough autonomy to deal with security issues in ways best suited to its individual environment.

According to Michail Bletsas, director of computing at MIT’s Media Lab and one of the volunteers contributing to MIT’s security team, “It [the security team] is extremely effective. I think it was one of the most successful efforts ever in IT here. We have never had to shut down our connections. For example, the SQL Slammer [worm] was dealt with in six hours, and that was on a Saturday night. There are a lot of smart volunteers who contribute to the cause.” Bletsas continued, “The more of us who play this role, the better it is for the university. I wouldn’t want to substitute the broad consensus that exists right now with the network security team with a rigid set of rules. This is a very fluid field right now, and one of the worst things you can do is set up rigid rules that everyone has to abide by.”

MIT also takes an interesting approach to confronting its constituents regarding IT security issues. According to James Bruce, “If you went to Johnny and said, ‘You did thus and so,’ he would deny it. If you say, ‘Someone is using your account to do thus and so,’ you will typically get an apology, and the activity will cease.” MIT takes this approach to notifying its users about violations of the institution’s IT security policies, and it has proven effective. Bruce said that over many years they’ve only once had a three-time offender who had to be referred to a disciplinary committee.

Jeffrey Savoy of the University of Wisconsin–Madison noted, “At a decentralized campus, controlling devices connected to the network is a challenge. Our process is that when a computer is hacked, it may be

taken off the network. Then, it will have to be audited by central security staff before it can be put back on [the network]. Repeat offenders have to go through a more thorough consultation with central security staff. First, we explain what we've done and then we explain how their compromised machine puts their campus colleagues at risk. We also educate the offender about what to do to prevent the compromise in the future, and most importantly, we obtain a commitment from them to perform the necessary security activities in the future."

Several research universities also noted that it is sometimes difficult to get faculty members to comply with security regulations, which, for example, require a compromised machine to be removed from the network until it is repaired. Philip Long described this situation and what Yale is doing to address it: "The most difficult situation is the researcher who is trying to get the research application in by the deadline the next morning and his machine is hacked into the night before. We block it from the Internet and he is upset because he says getting his grant application out is more important than protecting the network from a virus or hacker situation. But we are very sympathetic in that situation. We find a way to bring up his machine behind a firewall—we will bring up his machine behind it and let him relay what he needs to the Internet through this trusted machine—but we are not going to let his hacker on the network using his machine while he uses his machine to finish his work. We will also bring up the machine in a controlled environment, and he can copy files off of it."

Long, along with others who reported similar situations, indicated that this case is the exception rather than the norm. "More often what happens is that people will remediate their machines within 24 hours, because who wants to be off the network? We

call up people to inform them that there is a high school student from Toronto, Canada, logged into their machine and he is using it to mount a denial-of-service attack on Los Alamos, and they go, 'Oh my God!'"

## **IT Security Requires New Incentives**

Numerous IT security administrators we interviewed cited user adoption of IT security tools and techniques as an issue, especially at larger institutions where decentralization limits the direct control the central IT group has over systems and networks run by departments, schools, and researchers. These IT security professionals believe users generally want to help the institution to be secure but are often unsure how to do so. Another commonly held opinion among the IT security community is that end users' willingness to be secure is only good up to a certain point. If asked to do too much, in terms of either effort or knowledge, they will not readily comply.

Given the university community's apparent willingness to act securely if it proves convenient, institutions can take several approaches to make it easier for their users to behave in a secure fashion. Some of these are simple and low cost, whereas others require more effort to implement and maintain but also promise better returns. As Gregory Jackson, vice president and CIO of the University of Chicago, explained, "The more you make it easier for people to do the right things, the more successful you will be."

One simple approach is to create easy-to-follow instructions (or link to someone else's instructions) to secure commonly used systems and applications and make them easily available on the Web. Remind users that the updates and instructions are available, especially when a new operating system version is released or a new vulner-

ability is discovered. Similarly, institutions can create easy-to-understand versions of key security policies, along with IT security FAQs, and make them readily accessible to the community. The University of Texas at Austin has created such a site at <http://www.utexas.edu/computer/security>. It provides tips geared for both individual users and system administrators to help them secure their systems, and it has copies of all the institution's IT security-related policies in one place. The site also provides news on new security issues and a form for submitting questions to the university's IT security staff.

Another relatively simple approach is to provide links to commonly used IT security tools such as antivirus software, personal firewall software, or secure communications tools like SSH or SFTP from an internal Web site, making them easy to find and install. Many of the campuses we interviewed have site-licensed commercial applications like antivirus software and make them available to all users at no charge. By making it easy and cheap for users to find and install these applications, institutions substantially increase the chance that they will be used. Stanford University has developed such a site for its community at <http://www.stanford.edu/dept/itss/ess/>.

A somewhat more complicated approach is for the institution to create its own installers for commonly used operating systems and applications with all desired security modifications included and distribute them to campus system administrators and users on either an intranet server or physical media such as CDs. Another approach is to provide this type of "hardened" load-set on computers purchased through the campus computer store or a negotiated preferred vendor program. Tufts University has taken this approach, providing a customized load-

set that includes institution-specific security templates through a vendor agreement with Dell. Details on this program can be found by going to <http://ase.tufts.edu/its/tech.htm> and clicking on the "Dell Special Pricing" (department pricing) link.

Another, more complex, approach uses automated system configuration tools to monitor individual systems' configurations and automatically push updates out to them as necessary. This approach takes responsibility for at least some aspects of security management out of users' hands. This solution is common in the corporate world and is sometimes used in public computer labs at universities to ensure that systems remain configured as desired. However, its use does not appear to be widespread in higher education, perhaps because these are commercial systems requiring an upfront investment to purchase, or perhaps because the diversity of systems found at most colleges and universities makes the use of such a tool unwieldy. It might be feasible for institutions to consider an approach by which departments or individual users could sign up with central IT to participate in such a program, in return for a system management fee that would cover the program's cost. The institution could limit the operating systems and applications supported to make the program easier to manage.

A more resource-intensive version of the previous approach is for central IT to provide system management services on a charge-back basis to departments they don't normally support, as at least one institution we interviewed is doing. By taking this approach, they ensure that departments without access to professional IT support can have their systems managed by competent staff, reducing the institution's risk while leveraging their staff in areas like the help desk.

By implementing one or more of these suggested approaches and lowering the barriers for users and departments to make themselves more secure, institutions increase the likelihood that their community will make more of an effort to secure their systems and applications, increasing the level of security for the institution as a whole.

## Differences of Opinion

While the above lessons contain opinions shared among most institutions we interviewed for this study, we also noted several IT security areas where opinions differed on the appropriate course of action, even among leading institutions of similar size, mission, and complexity. This section expresses these differing points of view.

## Firewalls

Using perimeter firewalls as a first line of defense against potential cyber-miscreants has become the norm in most industries; the CSI/FBI 2002 survey shows 99 percent of respondents using firewalls. As shown in Chapter 4, only 70 percent of higher education institutions are using perimeter firewalls. However, for at least some of the institutions not using perimeter firewalls, this is not a lapse in security but rather a conscious strategy.

MIT's James Bruce expressed the "no perimeter firewall" view. "This is a university. For us, this means that the network pretty much has to be an open network. And so we pretty much don't believe in firewalls. The enterprise networking environment has no firewalls in it. Some departments will run firewalls—for example, genetic data and things of that nature—and the Lincoln Laboratory, which is part of the MIT address space, has a firewall, but for the most part, since our researchers like to explore new protocols, port assignments, and

new applications, trying to build a firewall is a fruitless endeavor. Just as soon as you build one, somebody wants to do something different, and you keep punching holes in it, and after a while it looks like Swiss cheese. So that means for us that the fundamental proposition is that our computers and our applications need to be secure. We focus on security at the individual machine level. We worry a lot about operating system security, about the bugs in operating systems, and we focus a lot on ensuring that our applications have appropriate levels of security, so indeed, we know who is making the transaction when the transaction occurs. We encourage people with computers to keep their operating systems at the current release and to make sure that all security patches have been applied."

Institutions like the University of Washington hold similar views. Other large research institutions, such as Indiana University, are beginning to evaluate perimeter firewalls but have not yet implemented them.

On the other hand, numerous institutions have installed perimeter firewalls and are pleased with the results. Paul Howell, information systems security officer at the University of Michigan, sees firewalls as one of the most effective IT security technologies an institution can deploy. "If you can install them and operate them correctly, they tend to be the key thing to go after because they tend to keep undesirable traffic from the Internet [from] washing up on your machines, [and] that can cause a lot of headaches."

San Jose State's Bruce Judd said, "You have to secure the network in two places—the core and the border. If those are well secured, then you can usually deal with everything in between." He continued, "[On our campus], every server and system service has to be registered with the firewall. Other servers are on private and unroutable

network segments. Now the only way you can get into a server in this private address space is through a VPN.”

South Dakota State’s Andrew Conley said, “We felt implementing the firewall is really effective because on our campus it blocked out a lot of people and scripts who are out there scanning. This approach has led to the biggest improvement of IT security at our institution.”

Analysis presented in Chapter 4 showed that the larger the institution, the less likely it was to have implemented a perimeter firewall and the more likely it was to use an interior firewall. The examples provided above suggest that campuses need to decide whether perimeter firewalls are a good fit for their culture and IT support capabilities.

Those who oppose perimeter firewalls feel they restrict their constituents’ ability to make free and open use of the campus network. However, to provide security, this approach needs to emphasize stronger measures at the individual system level, shifting the burden of support somewhat away from central IT and toward departments and individual users. On the other hand, installing firewalls requires IT organizations to be responsive to changing user demands and may also require awareness efforts, because having a firewall can sometimes cause lax security behavior among users. Either approach can provide adequate security, but one approach or the other may be a better fit for a particular institution’s needs.

## Policy

Institutions also have slightly differing opinions about the need for IT security policies and how comprehensive they need to be. As reported in Chapter 5, nearly 70 percent of responding institutions either have or are implementing some form of formal IT security policy, and only 8 percent

of institutions report that they have no IT security policy. We noted some opinion differences about what these policies should contain.

Indiana University is a good example of an institution with strong emphasis on IT security policies. Indiana has about 20 policies that cover IT security in some way. Its Information Technology Policy Office is responsible for creating and reviewing IT policies and educating the institution’s constituents about them.

Numerous institutions have not emphasized policy so much as part of their IT security efforts. When asked to describe his institution’s IT security policies, MIT’s James Bruce said, “MIT historically, and almost by intent, has fewer policies [in general] than most universities have. You will find some very simple network rules of use. However, more is done through [user] awareness than through policy.” The University of Washington is currently working on implementing its first formal IT security policies, although interim policies created by the IT organization have existed for some time.

While our analysis in Chapter 8 showed that having IT security policies does seem to make a difference, our survey research did not uncover the nuances of whether these policies were comprehensive (as at Indiana University), general (as at MIT), or unofficial (as at the University of Washington). From those institutions we interviewed for this study, we gathered that the decision as to which IT security policy route to take is largely cultural. If your institution tends to be policy driven, your IT security efforts will likely be more successful if you have strong, enforceable IT security policies. At an institution that is more policy averse, having strong IT policies may not be possible, and other approaches may need to be considered.