

10

Present and Future Alignment of Security Practices

It is found by experience that admirable laws and right precedents among the good have their origin in the misdeeds of others.

—Cornelius Tacitus

Since the first host computer at UCLA was connected to the ARPANET in 1969, both J.C.R. Licklider's vision of a "galactic network" and the practice of Internet networking have rested on principles of openness and accessibility. The Internet's earliest engineers at our colleges and universities built the current Internet following these principles. And much of what we have described in this study is the product of more than three decades of engineering and evolution guided by these principles. Openness and accessibility are at the core of higher education's Internet practice, regulation, and engineering. We can summarize this practice for most higher education institutions as follows: unfetter the Internet, rely on local policy and behavioral awareness, and secure the end points (desktops). The open Internet approach aligns well with the ideals of a democratic society, and certainly with those of higher education.

Today these principles and the open Internet are at risk because of increasing, persistent, and ever more malicious attacks on our networks. A major debate is commencing among information technology (IT) security professionals focusing on these

principles' merit and sustainability in the current environment and whether new or modified principles need to be adopted. Openness and accessibility are recognized as major factors contributing to the Internet's power to foster innovation. But increasingly they appear to place Internet security at too high a risk. Also, an open system depends on widespread awareness and behavioral self-controls on the part of network citizens. The current level of awareness and IT security practice on the part of the constituency does not appear to be commensurate with the current level of risk, leading IT security professionals to aggressively use available technologies as countermeasures. A new alignment of IT security with higher education's values, practices, and installed technologies may be needed and may already be occurring.

In a presentation entitled "Security in the Post-Internet Era," given at a workshop in Chicago on 12 August 2003, Terry Gray, director of networks and distributed computing at the University of Washington, squarely engaged this debate by offering a controversial thesis: "The open Internet is history, get over it." Gray based this assertion on

the observation that two recent Microsoft security vulnerabilities have forced most institutions and ISPs to embrace blocking of selected network services. Comcast, a major cable provider, has, for example, started blocking NetBIOS ports and is now blocking ICMP/ping. Almost everyone is now blocking the NetBIOS ports, if they weren't previously. In some Comcast areas, VPN (virtual private network) ports are also being blocked. On some campuses, there are frustrated, and probably exhausted, network administrators who favor blocking ports forever, contrary to their earlier and long-held belief in removing blocks.

Gray concluded that the new widespread vulnerabilities, combined with increased liability concerns, have brought us to a turning point, even in higher education. To his thinking, insecurities equal liabilities, which in turn will trump the concerns of network operators and users. Gray also argued that restrictive access policies resulting from these insecurities may impede innovation, the lifeblood of any college or university.

A fundamental shift in policy and practice toward a less open Internet will have profound implications for scholarly communications in higher education and IT security practices in colleges and universities. A key question is whether institutions can meet contemporary security requirements without undermining innovation, that is, whether innovation can find a way to flourish in spite of restrictive connectivity policies. If Gray is right, the pressure on the academy to align its values and beliefs with mainstream IT security practices will become irresistible. Some believe that academic values are inimical to IT security practices, and we will elaborate on these perceptions or "myths" about IT security on the basis of the study's findings. Gray's conclusions suggest that the moral arguments about what constitutes the free

exchange of scholarly ideas, right or wrong, are moot if they conflict with security requirements.

While the impulse to lock things down through unprecedented technical interventions is easy to understand amidst the mopping up of more than 150,000 infected machines in July 2003, there remain many advocates of continued openness on the Internet. Some, like Ken Klingenstein, project director of the Internet2 Middleware Initiative and chief technologist at the University of Colorado at Boulder, argued that a trend toward an Internet with only a few ports open and lots of other applications tunneled through those ports (port 80) is unsound policy and technically questionable. The debate is far from over.

In anticipation of IT security practice changes, we use our findings to suggest ways that higher education practitioners can align IT security with institutions' needs in this ever-changing environment. We elaborate on the changing environment and future trends that can be reasonably ascertained from our research. On the basis of these data, we suggest effective practices and strategies that build on the assumption of an open Internet. We also acknowledge that this key assumption may not be sustained.

IT Security Beliefs in Higher Education

This section presents some of the most commonly articulated beliefs (or leitmotifs) that create tension or operate as barriers to improving IT security in higher education. We look at both sides of arguments surrounding these beliefs. We present counterarguments that practitioners may be able to use at their institutions to overcome these barriers, whether they are indeed barriers or simply myths.

IT Security Inhibits Academic Freedom

One of the most frequently heard arguments against implementing stronger IT security at higher education institutions is that strong IT security is inimical to academic freedom. The concept of academic freedom embodies the right of faculty members and students to pursue controversial topics without censorship or the need for prior approval. The academic community needs open and unfiltered access to information resources to perform their teaching and research. There is a widely held perception that having strong, centrally managed IT security will somehow impinge upon this freedom.

Those who espouse this point of view seem to have several major tenets to their argument. First, they feel that having security in place would block their ability to do something, such as accessing resources or using a new technology. Second, they feel that by having to authenticate to the resources they access, their usage may be tracked and used against them in some way. Third, some feel that as academics, they should not be subject to standardization, regulation, or inconvenience when accessing institutional resources, including IT.

The viewpoint that IT security blocks access to resources, invades privacy, or introduces complexity or regulation likely derives from IT security technology, policy, and procedure implementations that are poorly aligned with the academic community's needs. It is certainly possible to create an IT security environment that introduces all of these problems and more. However, it is equally possible to create an environment in which IT security takes the academic community's needs into account.

If properly implemented, IT security can enhance academics' ability to access the

resources they want to access, when they want to access them, with little fear of being monitored. For example, an effective IT security program ensures access to institutional computing resources by preventing denial-of-service attacks, infection by computer viruses and worms, or other damage caused by hackers. It helps protect the data resident on institutional computers, thereby protecting the privacy of students, professors, and researchers by preventing unauthorized people from viewing their work or learning what information they have been accessing; and it ensures that their research is kept safe.

Technology alone is not the solution to creating such an environment. As with most complex technology implementations, policies and business decisions made when implementing the technology will dictate the results achieved. A firewall can be used to prevent all contact with the outside world or to limit the traffic that is allowed to pass through to an administrative computer, simultaneously leaving machines used for academic purposes largely open. Enlightened policies and procedures contribute to user confidence that academic freedom is being respected. Informing the academic community about IT security policies and demonstrating that the policy is being followed and can be trusted can alleviate many concerns about security's negatively impacting academic freedom.

We note that although academic freedom was the third most frequently cited barrier to IT security among our respondents, only 32 percent selected it as a barrier from a "choose all that apply" question format. This suggests that while this argument may be popular, most institutions may have figured out a way to work around or accommodate this concern.

IT Security Compromises Personal Privacy

Another commonly heard complaint about IT security is that it compromises personal privacy. In particular, when use of an authentication technology is required to access institutional resources, students and faculty fear that data is being collected on their activities and may later be used against them.

While tracking individuals' activities through their interactions with electronic systems has become endemic in today's society, ranging from the location of mobile phone calls to the use of ATM machines to the purchase of individual items at grocery stores, technology is just a tool that enables such tracking. Use of technology does not mandate that user information be tracked or that it be shared. Such decisions are driven by an organization's business needs, culture, and policies.

In many cases, the institution's business needs dictate that certain activities be tracked to ensure that institutional systems and information assets are being protected. For example, logs are kept of access to secure areas of the campus, if electronic keys are being used, to allow campus police to determine who was in a particular facility when a crime was committed. Log files are kept of changes to information such as student grades or financial transactions to protect against fraud.

However, organizations can take such tracking beyond what is necessary for business purposes. For example, it may be necessary for copyright protection to validate that a user trying to access an electronic publication is an active member of the university community prior to permitting access. But the institution has no reason to track the fact that a student is reading a right-wing political journal on a regular basis or that a foreign professor seems very interested in

articles about terrorist tools. Also, an institution probably has very little reason to track what Web sites a particular user has visited using a university network connection, although the capability to do so certainly exists. In situations where the business need is to determine whether a user is legitimate, we expect that most higher education institutions, rather than monitoring usage, will err on the side of collecting less information, to allay privacy concerns.

Again, having an accepted policy that explains what information the institution collects on its constituents, what the information will be used for, and when it is discarded can calm fears of the user community. And a well-conceived policy can prohibit an overzealous administrator from collecting information that does not enhance the institution's security but could compromise individual privacy.

A policy cannot be effective by itself. The institution must conduct awareness activities for users to ensure they understand and trust the policy and for staff members who configure and use security technologies. To further build confidence, the institution may wish to periodically audit the information being collected on its users and require business justification for any storage of personally identifiable information.

A close parallel to the issue of electronic surveillance and privacy exists in the library. Every time a library patron borrows a book, data linking the borrower and the book must be collected and stored until the transaction is completed and the book is returned, to ensure the university gets its book back. Does the library use this information to maintain records of what books individual students or faculty members have borrowed during their tenure with the institution? The library certainly has the capability to do so. Perhaps because this process has been around much longer than IT security tools, users are more

accepting of it, or take it for granted that their privacy is being protected. However, one does not often hear academics bemoaning their loss of privacy in the library, yet such cries can be heard in the IT security arena.

IT Security Limits Access to Information

Some users see firewalls, strong authentication technologies, secure application versions, and similar technologies as blocking access to online destinations, limiting their ability to collaborate with colleagues at other institutions, or restricting the technologies they can use. For example, our data show that 33 percent of baccalaureate institutions and 17 percent of doctoral institutions block some URLs through their firewalls.

Morrow Long, director of information security at Yale University, described Yale's approach to this issue: "When we close off access, we try to make sure it is not in conflict with the academic and research purposes of the university and the missions of the university. We have blocked off some things like Windows file sharing in the Internet for security reasons. We were very careful to publicize our decision and to obtain input from all members of the community. We made an alternative available to people who wanted to access PC hard drives from the Internet via a VPN. When we implement security, we try to make sure that it does not impede or impinge upon anything that people are doing or make sure that they have a chance to comment on it."

As with many other aspects of IT security, technology is only part of the picture. Configuration decisions and institutional policies and procedures play a much larger role than does the technology itself in determining whether deployment of a particular technology will cause users to lose access to some resource. Likewise, the purpose for which a

technology is deployed will largely determine how it affects users and their work. For example, a tightly configured firewall deployed at the perimeter of a research university's network might overly restrict some users' ability to access resources they need, yet the same device deployed to protect a particular network subnet hosting the university's administrative systems would have no such impact. Institutions that work with their communities to define solutions find that in many cases they can adequately balance the need for security with users' business needs.

Openness and Community Outreach Are at Odds with Security

The open sharing of information, both within and beyond the institution's walls, is part of many colleges' and universities' core mission. This need for openness often arises as an argument against adopting stronger IT security measures. Advocates of this position contend that security technologies would block their ability to share information within and beyond the institution.

When configured in a way that is aligned with the institution's academic and business needs, IT security tools and techniques should have minimal impact on the ability of faculty and students to openly share information with each other, with colleagues at other institutions, and with the world at large. We must ask, then, what exactly are we currently making available that we wouldn't be making available if we were more secure? In nearly all cases, the decision to implement stronger IT security will not change the types of information being made available, unless someone deems that particular items (such as research on biochemical agents) may only reach a restricted audience, given the data's sensitive nature.

Although institutions shouldn't need to significantly change the types of information shared and collaboration tools used, they might need to change how these activities are performed. For example, incoming Web traffic might be restricted to a certain set of servers for security purposes, requiring faculty members to publish their information on centrally managed Web servers rather than from departmental machines. Similarly, an institution might require that users employ secure versions of certain applications, say, SSH instead of Telnet, or SFTP instead of FTP, thereby providing a more secure environment without changing the functionality available to the end users.

A Transient Student Population is Difficult to Manage

Some believe that the "transient" nature of higher education's constituents complicates IT security management. Because a student's association with the institution often has a fixed duration, it is assumed that managing user accounts for a population with 25 percent or greater turnover per year is more difficult than similar tasks in other industries. Likewise, it is assumed that getting students to understand and comply with security policies and best practices is an ongoing and often futile effort compared with similar efforts in industry.

In reality, the issues faced by higher education regarding end-user turnover are similar to and may be easier to manage than those faced by industry. Although a transient population, students' tenure with the institution is predictable. Security staff can plan for a large influx of new users in late August or early September and assume they'll need to shut down a large number of user accounts after graduation each year. The user accounts affected by these changes are easily identifiable, and many institutions

have developed automated tools to let students activate their user accounts. Also, user account privileges for students tend to be very similar, making it easy to give students access to the systems they need. Some sectors of industry also face turnover rates of 20 percent and higher, but, unlike in education, such turnover is often less predictable and requires immediate termination of access rights, as the departing employees may have been fired or be leaving to go to a competitor.

A remaining issue is the institution's ability to get student users to comply with security policies and best practices. As we noted in Chapter 7, some institutions require that students read and prove they understand a simple set of acceptable use procedures before they can activate their user account. Others limit the institution's exposure to security vulnerabilities on student-managed machines by using firewalls for the residence halls, separating them from the rest of the campus network.

Faculty Autonomy Can Hinder Uniform IT Security Standards

Faculty members at colleges and universities are well known for their autonomy. The central administration at many institutions may have difficulty compelling their faculty and researchers to conform to rules and standards, particularly when some faculty perceive that such standards could impede their work. Moreover, at larger institutions, individual schools and even departments may operate with a significant degree of autonomy. Mark Yudof, former president of the University of Minnesota and now chancellor of the University of Texas System, once quipped, "Being president of a university is like being the managing director of a cemetery. You have a lot of people underneath you, but nobody listens."

Some institutions may have created IT security standards without regard for faculty needs, perceived or real. For example, requiring users to change passwords on administrative systems every 30 days works fine for staff members who use the system every day. But a faculty member who only accesses the system to enter grades once per semester probably sees such a policy as an imposition. Many faculty members value their ability to control the systems they use in their research and need flexibility to change their computing environment when necessary. Trying to fit such requirements into a framework designed for a corporate or administrative environment would be difficult at best.

To introduce security standards, IT security personnel must work with faculty members and their staff to make them aware of the need for security technologies, as well as their capabilities and limitations. They must design and implement standards flexible enough to accommodate both academic and administrative needs. This may be accomplished by setting broad standards such as “every computer connected to the network will run antivirus software,” rather than trying to dictate a particular brand and version. Thus, autonomous individuals or departments can develop solutions that best fit their needs.

Several respondents suggested facilitating IT security standards adoption by making it easy for autonomous users and departments to access centrally provided secure resources. For example, numerous institutions license antivirus software and make it available at no charge to the university community. Although users are not required to install this software, it is easier and cheaper than pursuing another alternative, and usage rates are high.

Using a slightly different approach, one institution centrally deployed Kerberos

and digital certificates for authentication purposes. Although the Kerberos principal was linked to the university’s central e-mail system, IT security personnel found that some users were not using their university-provided e-mail and therefore were not taking advantage of the additional security provided by the Kerberos/certificate-based authentication architecture. Many users didn’t know this technology was available or what its benefits were. To broaden its usage, the institution began requiring the use of a Kerberos principal to authenticate to critical business applications such as course registration or benefits enrollment. This substantially broadened Kerberos usage on campus without mandating that users employ a new technology just for security’s sake.

The Kerberos example also illustrates another key point about end users’ adoption of IT security tools and techniques. The easier the technology is to acquire and use, the more likely users are to adopt it. The ideal IT security environment would be nearly transparent to the end user, providing utility-like ease of use. Achieving such a level of transparency while providing adequate levels of security for the institution’s perceived risk level would mitigate many barriers to adoption of stronger IT security on our campuses. Through use of middleware technologies such as enterprise directories and role-based security, which enable easy-to-use features like single sign-on, institutions will be able to move closer to providing a more secure environment that their users will be willing to use.

Common Themes

In examining beliefs about IT security in higher education, we observed some common themes. First, some members of the academic community believe it is possible to deploy IT security tools and techniques in ways that cause problems for the university community, and, given the often broad ac-

ceptance of this belief, a good number of IT organizations probably have done so in the past. More important, however, with proper planning and design of IT security initiatives that take both the academic and the business needs of the university community into account, these myths do not have to become reality. As we have pointed out several times in this study, nontechnical factors including leadership, policy, education, and trust are essential components of an IT security architecture designed to protect and enhance rather than hinder a user's work at the institution. We also believe IT security discussions need to be conducted in layman's terms and focus on its impact on users as much as, and perhaps more than, its impact on the institution. And the discussion should involve representatives from all sectors of the institution.

Aligning IT Security with the Institution's Needs

Throughout this study, we have presented evidence that IT security is not just a technology issue. To be effective, IT security needs to encompass a strategy that is aligned with the institution's academic and business needs. Such a strategy needs to include the use of strong IT security technologies balanced with the people side of security, including strong leadership, effective policies and procedures, and awareness and training activities. Every institution has different needs, different resources, and a different starting point. Institutions must understand what threats they feel they need to protect against and develop an IT security program that addresses these threats in a way that does not adversely impact their constituents. This section presents some strategies, tools, and ideas that may prove useful to institutions starting down this path.

Balancing the Technology/People Equation

Our analysis indicates that many of IT security's "soft" components—leadership, policies and procedures, and training—have an appreciable impact on the perceived effectiveness of IT security. However, our research also found that many institutions focus much more on IT security's technology aspects than on the people side. When asked to describe their institution's IT security initiatives, many people we spoke with went into great detail about their firewalls, authentication tools, monitoring and scanning tools, and other technologies they had implemented. In most cases they gave fewer details about how awareness was handled or how policies and procedures were created, followed, and enforced. As presented in Chapter 8, when we asked survey respondents to identify barriers to implementing effective IT security at their institutions, only 10 percent pointed to technology, while awareness, for example, was an issue for 46 percent. In Chapter 5, we discovered that only 54 percent of respondents had formal IT security policies, fewer than 20 percent of institutions reported "often" to their senior management on IT security issues, and fewer than 40 percent had awareness programs in place for faculty, students, and staff.

On the basis of this evidence, we see an imbalance between IT security management's technical and people aspects at many institutions. While this is not quantifiable on the basis of the data collected for this study, our qualitative research suggests many institutions may be dedicating the bulk of their IT security resources to implementing and managing the technical aspects of IT security and allotting far fewer resources to managing the people aspects. However, the analysis presented in Chapter 8 indicates that institutions that have emphasized the cultural aspects of IT security management

feel that they are doing significantly better in managing their institution's IT security risks than those that have not. Although technologies are certainly an essential part of IT security, our analysis points to a need for institutions to strike more of a balance between technology use and people-oriented tools and techniques to make their IT security programs more effective.

Balancing IT Security Approaches

Figure 10-1 graphically depicts the issue of balancing technology and culture to create a balanced IT security approach. It shows four major strategies for securing an organization on the basis of the organization's strength in each area.

Reactive. A reactive organization will tend to have invested relatively little in either IT security technology or culture. This

is not to say that the organization has left itself wide open to all threats, but it has not implemented a full spectrum of leading-edge technologies or leading practices for creating a secure culture. An organization pursuing this approach is likely to invest in IT security on the basis of incidents rather than as part of a strategic plan.

Cultural. Organizations emphasizing a cultural approach to security focus their efforts on creating a culture of security. By instilling awareness of security issues into their workforce, creating and disseminating comprehensive policies and procedures, and training their users, they hope to be able to avoid the many security vulnerabilities caused by human error and limit their investment in technology.

Technology-centric. This approach relies primarily on technical means such as firewalls, scanning tools, intrusion detection

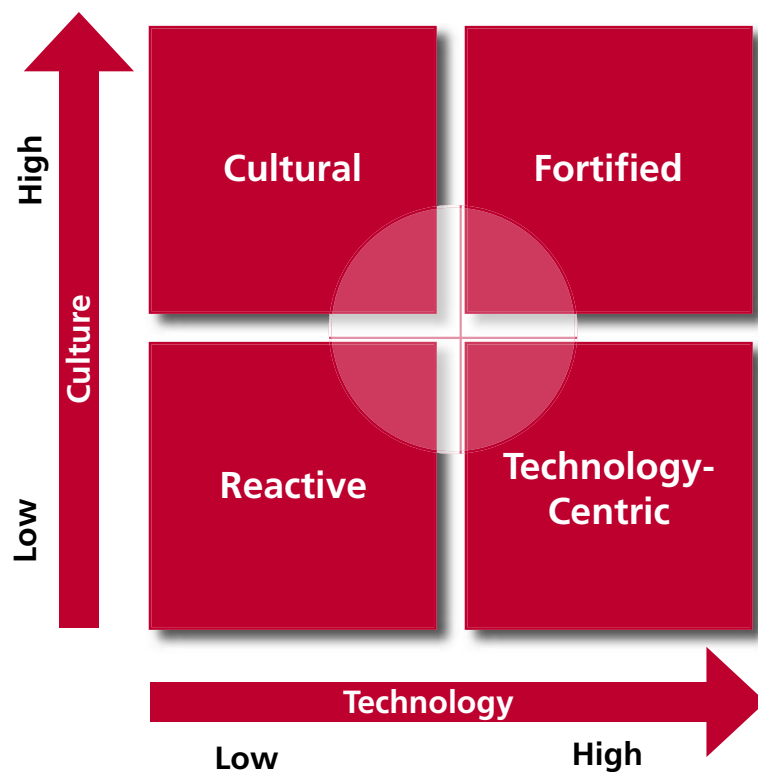


Figure 10-1. IT Security Approaches

systems, and complex authentication and authorization systems to secure IT assets. Highly decentralized organizations or those without strong executive sponsorship may be more likely to use such a strategy.

Fortified. A fortified strategy encompasses both strong IT security technology and a security-oriented organizational culture. Organizations using such a model will generally do so as part of a conscious plan, as this approach would be difficult to arrive at through an evolutionary path. Those choosing such a model probably tend to do so because they perceive themselves to be at high risk from IT security issues; because some external requirement, such as HIPAA (the Health Insurance Portability and Accountability Act), has led them there; or because security is a concern for one or more of their senior executives.

Note that this model is not intended to be prescriptive. An institution might find any one of these strategies appropriate, depending on factors such as perceived risk, available resources, institutional culture, and executive leadership. Also, these strategies are not absolute and can be pursued to varying degrees. So, for example, an institution choosing a reactive strategy could choose to be technically reactive (farther to the right on the technology axis), culturally reactive (closer to the top on the culture axis), or balanced (toward the center of the diagram). We feel that regardless of the strategy chosen, many institutions will move toward a balanced approach, represented by the shaded circle in the diagram's center, because such an approach offers a good mix of effective technical and cultural solutions to IT security issues while limiting the resources needed to execute the strategy. Also, the more balanced the approach, the more likely it is to align with the institution's academic and business needs.

Today, we feel that many, although not all, higher education institutions are in the technology-centric quadrant. Several factors may account for this. First, IT security does not appear to be high on most institutions' executive agenda: fewer than 40 percent of responding institutions had a neutral or better opinion that their president or provost participated in the creation of their IT security policies, and fewer than 15 percent frequently reported on IT security to the institution's senior management. Fully 95 percent of our respondents indicated that IT security reported to the CIO or other IT manager.

Without strong executive support, IT security organizations often find it difficult to get their constituents to pay attention to training and awareness efforts, to set standards, or to enforce policies. As one senior IT security officer at a large research university stated, "The problem we have with [IT security] education around here is getting people to pay attention. Communication in our environment is very difficult, because we have many vehicles for communication, and people can ignore them all." And because IT management has responsibility for IT security initiatives, they may tend more toward the known realm of technology solutions and less toward the more difficult cultural approaches.

A second major factor contributing to higher education's technology-centric bent may be the availability of resources to manage and enhance security. Every organization must implement a certain degree of technology (such as authentication and virus protection) to adequately protect its users and assets from common threats, and in some cases, resources may not be available to progress far from this baseline.

As described in Chapter 8, nearly 72 percent of respondents cited resource availability as a barrier to IT security at their

institution, and this view was backed up at many of the institutions interviewed as part of this study. As one IT security officer said, "We're in a time of budget reductions, and it is hard to make the case [for more people]. Without the people, customer service will suffer first." Carol Myers, director of ITS Security Services at the Maricopa Community Colleges, concurred. "Our technical work has been more successful than our training and awareness [activities]. We lack the budget for them." When asked, "If you received additional resources for IT security, how would you invest them?," many IT security managers interviewed indicated that they would like to invest more heavily in user awareness and education and to make their institution deal more proactively with IT security issues.

Understanding and Managing Risk

Illustrating the need for a balanced IT security approach, Figure 10-2 presents

one simple model for evaluating the types of security risks an institution could face and outlines some common approaches used to combat each type of threat. Note that for clarity, the figure omits approaches that could be used against all threat categories, such as authentication and authorization tools and antivirus software.

Using this model, institutions could address four different risk categories.

Internal and accidental. This category encompasses internal users' unintentional security breaches, such as using a blank or easily guessed password, storing confidential data on an insecure system, or giving out their passwords to someone over the phone. Such security breaches are difficult to combat because automated tools cannot easily prevent human error. To mitigate these risks, institutions need to develop policies and procedures to guide internal users as to what they should and should not do in

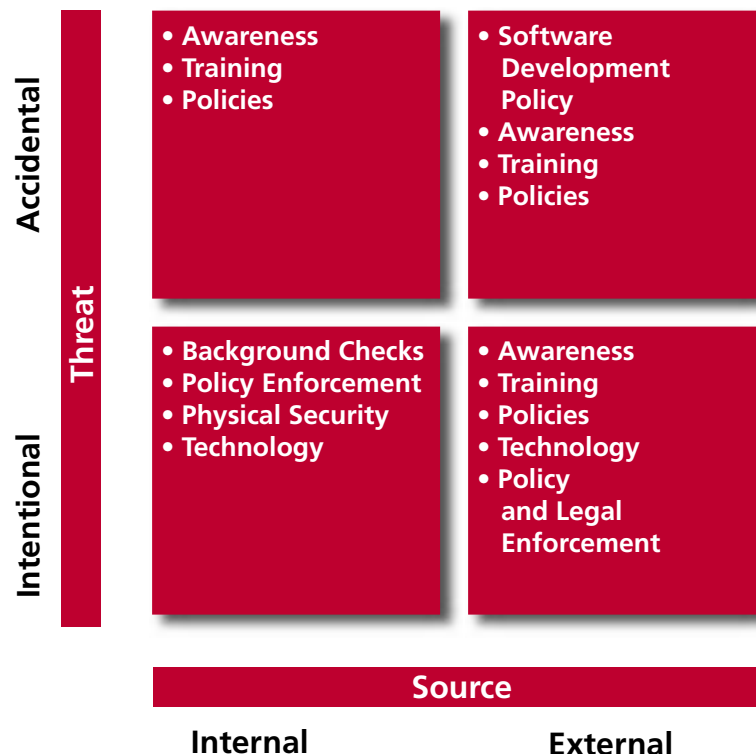


Figure 10-2. Risk Assessment and Response

particular situations, train users on these policies and procedures, and continually offer awareness activities to ensure that users are conscious of new threats and will remember to act securely.

External and accidental. This somewhat rare type of threat occurs when an external user somehow gains access to a system or information they were not supposed to be able to see. An example could be a Web-based application that asks for an ID number and returns personal information on an individual without authenticating the user's identity. One author of this study, required to provide his Social Security number online to an institution as part of a conference registration process, refused to do so and entered 111-11-1111, only to find that number and similar numbers had been taken. In frustration, he then put in a random number that accidentally matched a real number in the system, which in turn caused the system to provide all kinds of personal information about an earlier subscriber. Notified of the system design failure, the institution, quickly and with appreciation, fixed the system. The primary tools for defending against such exposure are policies and procedures, especially those that incorporate security into system design and testing, along with awareness and training activities geared toward ensuring that confidential information is not left exposed to unintended users.

Internal and intentional. Intentional attacks from internal users are not uncommon and could occur for reasons including personal gain, revenge against a perceived wrong by a colleague, supervisor, or professor, or just the thrill of doing it. IT security technologies such as internal firewalls, strong

authentication mechanisms, data encryption, and intrusion detection tools can help the institution protect against such threats. Additionally, criminal background checks of employees with access to sensitive information, clear mechanisms for IT security policy enforcement, and physical security around key systems can help the institution protect itself against such threats.

External and intentional. Most people think of this attack type when they hear about an IT security breach: a willful attack by an external hacker. Again, IT security technologies such as perimeter and internal firewalls, strong authentication mechanisms, data encryption, and intrusion detection tools can help protect the institution against such threats. Likewise, policies and procedures that focus on detecting and reacting to external threats, cooperating with law enforcement, and removing compromised systems from the institution's network are important tools against such threats, as are user awareness and training.

This model helps demonstrate the need for an IT security approach that balances security's technological and cultural aspects. It shows, for example, that technology can help protect against intentional threats but is less effective against accidental ones. Similarly, cultural tools such as policies, procedures, and awareness provide a strong defense against accidental exposures and complement technology to provide a stronger defense against intentional threats.

Developing a Business Case for IT Security

Institutions can develop a business case for IT security using a simple model, such

as Figure 10-3. This model profiles and compares risks and effectively presents them to nontechnical management. One axis represents the perceived risk to the institution, which could include factors such as the number of times the risk has been observed, defense mechanisms currently in place to defend against that risk, and potential damage (both financial and otherwise) to the institution should the risk become reality. The second axis, implementation difficulty, could encompass cost and level of staff effort to implement a solution, along with the cultural resistance a solution might face.

Ranking potential IT security initiatives in this way yields four major categories.

Discretionary improvements are easy to implement but address low-risk issues. Institutions may choose to implement these recommendations over time, on the basis of resource availability.

Low-value initiatives are difficult to implement and address a low-risk issue. For

such initiatives, institutions might conduct additional analysis to determine whether the effort necessary is worthwhile, given the low incremental benefit it provides. Institutions may also wish to defer the implementation of these initiatives until a later date, or choose not to implement them at all.

Quick wins address high-risk areas and would not be difficult to implement. Institutions would likely want to implement solutions for all risks that fall into this category as quickly as possible.

Necessary projects address a high-risk area but require a high level of effort to implement. Because they are probably necessary to implement, their difficulty means they need to be treated as distinct projects. Institutions may wish to further prioritize the implementation of initiatives in this category by balancing the risk's immediacy against the availability of resources to correct the issue.

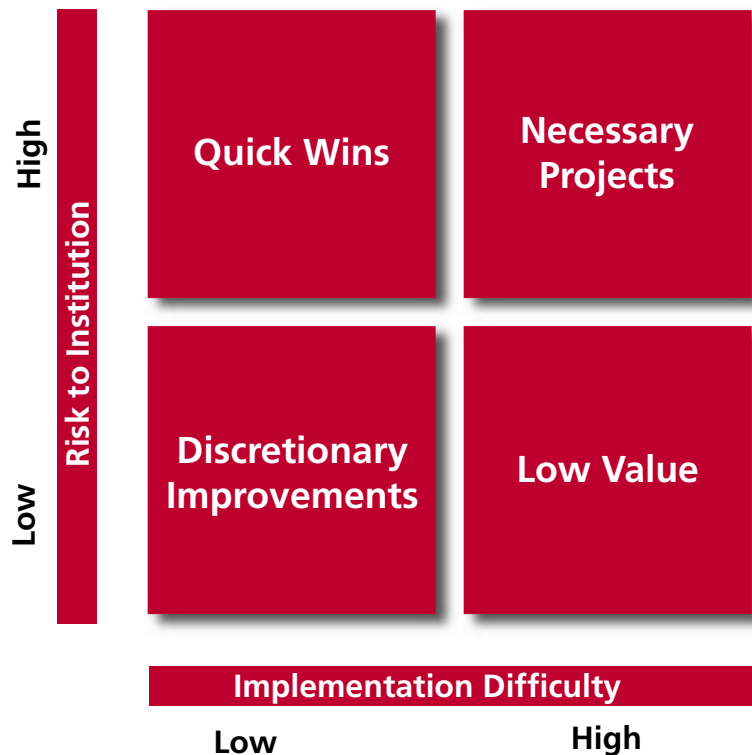


Figure 10-3. IT Security Risk Analysis Framework

The Changing IT Security Environment

The IT security arena has been the Wild West of the information technology field for the last decade. Since the explosion in Internet usage in the mid-1990s, the IT security field has changed rapidly, moving faster than the legal environment, technology vendors, and many IT practitioners themselves have been able to react. However, in the past several years, the environment itself has started to change, both for better and worse. Terry Gray captured some of these changes and their ramifications in his provocative presentation, discussed earlier. Among the changes he noted were greater reliance on self-imposed denial-of-service, firewalls everywhere, more tunneled traffic through fewer ports, and more difficult troubleshooting.

The legal system has begun to understand cyber crime and is starting to define what constitutes a crime in the online world and to set real penalties for malefactors. However, as with anything new, some feel that the emerging laws have swung the pendulum too far in the other direction and that the laws will require some tweaking to be administrable and effective.

Technology vendors are beginning to understand that security is an important part of their product offerings. Some have begun to integrate security into their products, although there is still a long way to go, particularly for vendors of desktop operating systems. Indeed, vendors could and should use higher education's needs and open environment as a testing ground as they continue to develop products for broad end-user application. In many ways, the higher education environment mirrors the world of most private Internet users.

And IT professionals have also begun to change, with IT security officers becoming

members of a distinct profession with its own certifications, toolsets, and responsibilities. However, even as the IT security area matures, one thing will likely stay the same for some time to come: rapid change.

Technology

IT security technologies have changed significantly since the early days of IT security. Whereas higher education IT security visionaries once had to develop their own tools to secure their systems (for example, MIT's creation of the Kerberos authentication toolset in the 1980s), today IT security professionals have a wide variety of tools available from a huge number of vendors and the open-source community. These tools' sophistication continues to increase, as does their ease of use, bringing more powerful capabilities to institutions without large IT departments.

Institutions must continue to take advantage of IT security technologies' new capabilities because, as with any arms race, the tools available to the hacker community are also evolving rapidly. This will likely increase the pool of potential attackers because the availability of automated, freely distributed tools that exploit known vulnerabilities in commonly deployed operating systems and applications brings ever greater capabilities to hackers who need increasingly less knowledge to operate these tools. Bruce Judd, associate vice president for university computing and telecommunications at San Jose State University, succinctly described this challenge: "This is a cat-and-mouse game. Hackers are always getting better, as are my tools to deal with them."

Legal Environment

As the legal system begins to catch up with the advances of the Internet Age, new legislation will likely help IT security manage-

ment in the long term, although it is creating near-term headaches for many institutions.

At the federal level, laws like HIPAA and FERPA (the Family Educational Rights and Privacy Act) change the IT security equation for many institutions. Both of these laws contain specific provisions governing the privacy of certain types of data and, in the case of HIPAA, contain specific rules for IT security at institutions dealing with health-care data. Both laws up the ante for compliance with IT security provisions as well, and large fines and jail time are possible for violations. In addition to these federal regulations, some states, such as California, are also passing IT security legislation.

The legal environment promises to get more complex as new initiatives around homeland security, identity theft, spam e-mail, and other hot issues will likely continue to impose new requirements on IT security professionals. As some health-care organizations have done in response to HIPAA, institutions may be able to turn legislation-mandated changes into an opportunity to revamp their IT security capabilities and community practices, rather than trying to meet the requirements with their existing IT security architectures and policies. John Houston, privacy officer and director of IS for the University of Pittsburgh Medical Center, said, "A lot of what they are telling us to do under the [HIPAA] security rule are really things we needed to do anyway."¹

Changing Nature of Threats

Another significant issue facing the IT security community, and one that may cause many institutions to rethink how they manage IT security, is the changing nature of the threats they face. Jeffrey Schiller, network manager at the Massachusetts Institute of Technology, explained, "The nature of the

problem is changing. In the past, we faced individual bad guys trying to break in. Now, we are dealing with worms, bots, and zombies—automated attacks. A machine with a vulnerability will be exploited in a matter of hours. This stuff does not stop for weekends, holidays, or anything else."

Another issue institutions need to face is that the reasons for attacks also may be changing. In the past, many hackers who broke into university computer systems did so just because they could or because they wanted access to the system to use it to attack another system. Today's attackers seem to have more-nefarious plans: they attempt to use worms or other means to take control of large numbers of computers and then use them to launch distributed denial-of-service attacks against other entities. For example, in August 2003, hackers compromised at least 2,400 computers at Stanford University by exploiting a known (and patchable) hole in the Windows operating system. Although the infection was discovered before the machines were used to attack other systems, it still cost the university significant time and effort to clean and patch all of the machines.² Identity theft is also causing growing concern, and universities may be increasingly targeted because they hold personal data for large numbers of students and employees.

Future Trends

It is impossible to accurately predict the future, and given the rapid changes in the IT security space, it would be foolish to try to prognosticate about tactical-level changes institutions will face in the coming years. However, from our research and interviews, we were able to discern some higher-level trends.

Technology Trends

In Chapter 4, we profiled the technologies institutions have already installed and their plans for future deployments. When analyzing this data, several trends emerge. First, institutions as a whole continue to implement core security technologies, such as SSL for Web transactions and perimeter firewalls. More than 70 percent of our respondents have such technologies in place today, and within one year, 88 percent plan to have implemented these technologies, with the numbers going above 92 percent within two years. Second, institutions plan to accelerate the pace of implementing more advanced security technologies. For example, only 48 percent of institutions reported having an enterprise directory in place at the time they were surveyed, but 86 percent plan to have such a system in place within one year, and 94 percent within two years. Other rapidly growing technologies include intrusion prevention and detection tools, encryption, and VPNs, the use of which will grow at nearly a 40 percent pace over the next year.

Finally, planned use of emerging security technologies seems to be more measured. For example, only 1 percent of institutions were using technologies like Shibboleth or biometric authentication at the time of our survey. Within one year, 17 percent of institutions plan to be using Shibboleth, and 6 percent plan to be using biometrics; within two years, the figures rise to 41 percent for Shibboleth and 24 percent for biometrics. These growth rates suggest that higher education is cautious about implementing new technologies, although institutions do recognize the need and plan to use them in the future.

As institutions continue down the path of implementing many traditional security technologies, the world of IT security continues to evolve rapidly, with both the

sophistication of threats and the power of tools designed to combat them increasing quickly. In such a rapidly changing environment, there is some concern that traditional security technologies might need to yield to new paradigms for keeping organizations secure. Ken Klingenstein espoused the viewpoint that “newer [IT security] technologies may not be a fit with older designs.”

One such paradigm shift is the increasing use of middleware—software that facilitates interactions between disparate computer systems—to deal with the ever-increasing complexity of relationships between systems, individuals, and organizations. Examples of middleware IT security solutions include enterprise directories, which can pass one set of authentication credentials for a user to multiple systems within an institution's network; role-based security for authorization, which provides users access to certain applications and data in multiple systems on the basis of their role(s) in the organization; and Shibboleth, a new open-source technology that allows cross-organizational sharing of attributes about users.

Increased Accountability

IT security is quickly moving from an issue relevant only to technologists to an everyday concern for people in all walks of life. Issues such as identity theft are becoming fixtures on the nightly news, and efforts to combat music piracy, spam, and other nuisances and new cyber crimes make headlines every day. As a result, institutions will be under increased pressure from their constituents to provide robust IT security as awareness of its importance rises.

University students and employees will not be the only ones to notice IT security's increased importance. Politicians at both the federal and state levels have begun to tackle IT security issues, and, as we discussed earlier in this chapter, new laws with real penalties

for violations are emerging that will force institutions to rethink their approach to IT security management. Finally, pressure will likely emerge from institutional business partners. For example, credit card companies require that organizations accepting their cards provide minimum levels of security. Similar expectations could increase from other key partners, including grantors of financial aid and research dollars.

In this environment, experiencing an IT security failure will do more than give the institution a short-lived black eye. Emerging legislation provides for stiff fines and possible jail time for violators, and it is probably only a matter of time before civil litigation for personal information exposure becomes rampant. While this environment will require all organizations, including universities, to improve their IT security environments, the increasing accountability will also likely make IT security more of an executive-level concern, making it easier for IT security managers to obtain the resources they need to make these improvements.

Centralization and Standardization

As the complexity of security issues and technologies grows, and as the time available to deal with threats decreases because of the automated nature of many new attacks, individual departments and research labs within institutions will in many cases have neither the funding nor the expertise to maintain their own IT security. This, in turn, may precipitate a move to more standardized and centralized IT security management at large institutions. Likewise, at some institutions, the increased spotlight on IT security may result in a mandate from senior management to consolidate IT security operations in a professional IT security organization to reduce the institution's risk exposure.

Some institutions have already begun to offer centralized IT security management services to their communities, although their use is not mandated at this point. For example, the University of Michigan has begun to implement a centrally managed logical firewall system. Paul Howell, information systems security officer, explained, "I have been working closely with some of the network engineers on campus. We have come up with a technical solution that creates the appearance of a firewall—a logical firewall. We are working with several novel firewall products. We are able to give the illusion to a group that they have a firewall dedicated to them and that they administer [it] and no one else can fuss with it; no one else can see the policy and the logs. But in actuality they are operating a virtual firewall that exists on a shared resource that is hosting many firewalls—like a single machine that hosts a half-dozen Web domains."

At San Jose State University we found another example of a centrally managed service designed to improve security. As part of its recent enterprise resource planning system implementation, the institution was left with an underutilized mainframe system. Rather than decommission the system, in partnership with IBM they reconfigured the mainframe to provide virtual Linux servers to the campus. Bruce Judd said, "We are the first university to provide those in a large scale to individual faculty at no cost." In addition to these virtual Linux servers, Judd's team has provided an Oracle database site license and assorted open-source applications. As a result, they hope to convince faculty members to use this professionally managed system rather than setting up and maintaining their own teaching and research systems.

Sharing the Burden

As the demand for IT security continues to grow, many institutions, especially smaller

ones, may find themselves overwhelmed by the level of resources needed to keep up. As a result, we anticipate that smaller institutions may turn outside for a solution. One answer may be to collaborate with other small institutions, forming partnerships or consortia to develop shared IT security management capabilities. Martin Smith, chief information officer at Embry-Riddle Aeronautical University, expressed this view. "Schools are going to form consortia. We are talking with some of our local schools about forming a consortium to deal with security and disaster backup. No school can afford to do it themselves, with money and budgets tight in the state and private schools." Another alternative may be to turn to managed security services vendors to handle the bulk of day-to-day IT security management.

While some institutions are looking to collaborate on developing IT security management capabilities, others are coming together to develop new IT security solutions. For example, several major research universities are jointly sponsoring Shibboleth, a toolset designed to let institutions share access controls for Web resources. We expect such efforts to continue as institutions try to develop solutions to some of higher education's IT security needs.

Conclusion

This study's quantitative and qualitative data suggest that many higher education institutions provide levels of IT security that

are roughly on par with their counterparts in the corporate world, despite a perceived lack of resources and some unique differences and challenges they face. However, the data indicated that some institutions still have a long way to go in providing high-quality IT security services.

Our results also indicate that while many institutions have implemented a range of technologies to combat IT security threats, far fewer use awareness programs and the acceptance of comprehensive IT security policies and procedures to resolve cultural issues that impact IT security. And somewhat surprisingly, IT security does not appear to be an executive-level issue at many institutions.

Colleges and universities face some significant challenges in implementing IT security, including resource constraints, ever-increasing threats, a changing legal landscape, and rapid technology advancements. And while universities and colleges must undergo some degree of change to overcome these obstacles, our data indicate that the higher education community is rising above these challenges and providing a secure teaching, research, and business environment for its constituents.

Endnotes

1. A. Dragoon, "Eight (Not So) Simple Steps to the HIPAA Finish Line," *CIO Magazine*, 1 July 2003, p. 74.
2. See <<http://news-service.stanford.edu/news/2003/august20/hackers-820.html>>.